D-Link®

DES-3225G Series 24-Port Fast Ethernet Switch User's Guide

Fourth Edition (September 2000)
65153225G045
Printed In Taiwan

RECYCLABLE

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a – Netzkabel oder Netzstecker sint beschädigt.
    b – Flüssigkeit ist in das Gerät eingedrungen.
    c – Das Gerät war Feuchtigkeit ausgesetzt.
    d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht gr□ßer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS
D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contactin

g a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address/telephone/fax/e-mail/Web site list of D-Link offices is provided in the back of this manual.

Trademarks

Copyright ©2000 D-Link Corporation. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist in Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

注意

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Warning

警告使用者

這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,在這種情況下使用者會被要求採取某些適當的對策.

Table of Contents

INTRODUCTION 1

FAST ETHERNET TECHNOLOGY 1
GIGABIT ETHERNET TECHNOLOGY 1
SWITCHING TECHNOLOGY 2
FEATURES 2
Ports 2
Performance features 3
Management 3

UNPACKING AND SETUP 4

UNPACKING 4
INSTALLATION 4
Desktop or Shelf Installation 5
Rack Installation 5
POWER ON 6
Power Failure 6

IDENTIFYING EXTERNAL COMPONENTS 7

FRONT PANEL 7
REAR PANEL 7
SIDE PANELS 8
OPTIONAL PLUG-IN MODULES 8
100BASE-TX Module 9
100BASE-FX (SC) Fiber Module 9
100BASE-FX (MT-RJ) Fiber Module 9
1000BASE-SX Gigabit Module 10
1000BASE-LX Gigabit Module 10
1000BASE-T Copper Gigabit Module 11
LED INDICATORS 11

CONNECTING THE SWITCH 13

SWITCH TO END NODE 13
SWITCH TO HUB OR SWITCH 13
10BASE-T Device 14
100BASE-TX Device 14

SWITCH MANAGEMENT CONCEPTS 15

LOCAL CONSOLE MANAGEMENT 15
Diagnostic (console) port (RS-232 DCE) 15
IP ADDRESSES AND SNMP COMMUNITY NAMES 16
TRAPS 16
MIBS 17
PACKET FORWARDING 17
Aging Time 18
Filtering Database 18
SPANNING TREE ALGORITHM 18
STA Operation Levels 19
On the Bridge Level 19
On the Port Level 19
User-Changeable STA Parameters 19
Illustration of STA 20
PORT TRUNKING 21
VLANS AND BROADCAST DOMAINS 22

MAC-based Broadcast Domains *23*
802.1Q VLANs *23*
802.1Q VLAN Segmentation 24
Sharing Resources Across 802.1Q VLANs 24
802.1Q VLANs Spanning Multiple Switches 25
Port-based VLANs *26*
BROADCAST STORMS 27
Segmenting Broadcast Domains *27*
Eliminating Broadcast Storms *27*

USING THE CONSOLE INTERFACE 28

SETTING UP A CONSOLE 28
CONNECTING TO THE SWITCH USING TELNET 29
CONSOLE USAGE CONVENTIONS 29
FIRST TIME CONNECTING TO THE SWITCH 29
User Accounts Management *31*
Saving Changes *31*
LOGGING ONTO THE SWITCH CONSOLE BY REGISTERED USERS 32
Create/Modify User Accounts 32
View/Delete User Accounts 34
SETTING UP THE SWITCH 35
Configuration *35*
Configure IP Address 36
Configure Console 38
Configure Switch 39
Configure Ports 40
Configure Slot1 Module 42
Configure Slot2 Module 44
Configure Port Mirroring 45
Configure Spanning Tree Protocol 46
Configure Filtering and Forwarding Table 49
Configure IGMP Filtering 52
Configure VLANs & MAC-based Broadcast Domains 56
Configure Trunk 77
Update Firmware and Configuration Files *78*
System Utilities *79*
Ping Test 80
Save Settings to TFTP Server 81
Save Switch History to TFTP Server 82
SNMP Manager Configuration *83*
SWITCH MONITORING 84
Network Monitoring *85*
Traffic Statistics 85
Browse Address Table 91
Browse IGMP Status 92
Browse GVRP Status 93
Browse GMRP Status 94
Switch History 94
RESETTING THE SWITCH 95
Restart System *95*
Factory Reset *96*
Logout *97*

WEB-BASED NETWORK MANAGEMENT 98

INTRODUCTION 98
GETTING STARTED 98
MANAGEMENT 98
Configure Switch *99*
IP Settings 100
Port Settings 101
Port Mirroring 103

Switch Settings 104
Filtering and Forwarding Table 106
Spanning Tree 113
IGMP Filtering 116
VLANs & MAC-based Broadcast Domains 118
Trunk 126
Configure Management *126*
Traps and Community Strings 127
User Accounts 128
Console Port Settings 130
Monitor *131*
Switch Overview 131
Port Statistics 132
Browse Address Table 137
Browse IGMP Status 141
Browse GVRP Status 142
Browse GMRP Status 143
Switch History 144
Reset and Update *144*
Reboot Switch 145
Reset to Factory Default 146
Update Firmware 147
Change Configuration File 148
Save Settings to TFTP Server 149
Upload Log File 150
Save Changes *151*
Help *151*

TECHNICAL SPECIFICATIONS 152

RJ-45 PIN SPECIFICATION 155

SAMPLE CONFIGURATION FILE 157

Commands: 157
Notes about the Configuration File: 158

RUNTIME SWITCHING SOFTWARE DEFAULT SETTINGS 159

INDEX 160

ABOUT THIS GUIDE

This User's Guide tells you how to install your DES-3225G Series Switch, how to connect it to your Ethernet network, and how to set its configuration using either the built-in console interface or Web-based management.

Terms

For simplicity, this documentation uses the terms "Switch" (first letter upper case) to refer to the DES-3225G Series 24-port NWay Ethernet Switch, and "switch" (first letter lower case) to refer to all Ethernet switches, including the DES-3225G.

Overview of this User's Guide

- Chapter 1, "*Introduction*." Describes the Switch and its features.
- Chapter 2, "*Unpacking and Setup*." Helps you get started with the basic installation of the Switch.
- Chapter 3, "*Identifying External" Components*. Describes the front panel, rear panel, optional plug-in modules, and LED indicators of the Switch.
- Chapter 4, "*Connecting the Switch*." Tells how you can connect the DES-3225G to your Ethernet network.
- Chapter 5, "*Switch Management Concepts*." Talks about Local Console Management via the RS-232 DCE console port and other aspects about how to manage the Switch.
- Chapter 6, "*Using the Console Interface*." Tells how to use the built-in console interface to change, set, and monitor Switch performance and security.
- Chapter 7, "*Web-Based Network Management*." Tells how to manage the Switch through an Internet browser.
- Appendix A, "*Technical Specifications*." Lists the technical specifications of the DES-3225G.
- Appendix B, "*RJ-45 Pin Specifications*. Shows the details and pin assignments for the RJ-45 receptacle/connector.
- Appendix C, "*Sample Configuration File*."
- Appendix D, "*Runtime Switch Software Default Settings."*

1

INTRODUCTION

This section describes the features of the Switch, as well as giving some background information about Ethernet/Fast Ethernet, Gigabit Ethernet, and switching technology.

Fast Ethernet Technology

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-TX, provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The dominating market position virtually guarantee cost effective and high performance Fast Ethernet solutions in the years to come.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100Mbps Fast Ethernet and a one hundred-fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential to coping with the network bottlenecks that frequently develop as computers and their busses get faster and more users use applications that generate more traffic. Upgrading key components, such as your backbone and servers to Gigabit Ethernet can greatly improve network response times as well as significantly speed up the traffic between your subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. And with expected advances in the coming years in silicon technology and digital signal processing that will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, outfitting your network with a powerful 1000Mbps-capable backbone/server connection creates a flexible foundation for the next generation of network technology products.

Switching Technology

Another key development pushing the limits of Ethernet technology is in the field of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by making it possible for a local area network to be divided into different *segments* which don't compete with each other for network transmission capacity, giving a decreased load on each.

The switch acts as a high-speed selective bridge between the individual segments. Traffic that needs to go from one segment to another (from one port to another) is automatically forwarded by the switch, without interfering with any other segments (ports). This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

For Fast Ethernet or Gigabit Ethernet networks, a switch is an effective way of eliminating problems of chaining hubs beyond the "two-repeater limit." A switch can be used to split parts of the network into different collision domains, for example, making it possible to expand your Fast Ethernet network beyond the 205-meter network diameter limit for 100BASE-TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks.

Switching LAN technology is a marked improvement over the previous generation of network bridges, which were characterized by higher latencies. Routers have also been used to segment local area networks, but the cost of a router and the setup and maintenance required make routers relatively impractical. Today's switches are an ideal solution to most kinds of local area network congestion problems.

Features

The DES-3225G Switch was designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continuously.

Switch features include:

Ports

- 24 high performance NWay ports all operating at 10/100 Mbps for connecting to end stations, servers, and hubs (22 MDI-X 10/100 Ethernet UTP ports and 2 MDI-II Uplink ports).
- All ports can auto-negotiate (NWay) between 10Mbps/ 100Mbps, half-duplex or full duplex and flow control.
- One optional rear panel slide-in module interface for a 1-port 1000BASE-SX Gigabit Ethernet module, a 1-port 1000BASE-LX Gigabit Ethernet module, or a 1-port 1000BASE-T Gigabit Ethernet module, for connecting to another switch.
- One slide-in module interface in the front panel for 1 or 2 port 10/100M Ethernet connection. Three modules are available: 2 ports TX module, 2 ports FX MT-RJ type module, and 1 port FX SC type module.

- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

Performance features

- Store and forward switching scheme capability to support rate adaptation and protocol conversion.
- Full- and half-duplex for both 10Mbps and 100Mbps connections. The 1000BASE-SX and 1000BASE-LX Gigabit Ethernet modules operate at full duplex only while the 1000BASE-T Gigabit Ethernet module can also operate in half-duplex mode when auto negotiate is selected. Full duplex allows the switch port to simultaneously transmit and receive data, and only works with connections to full-duplex capable end stations and switches. Connections to hubs must take place at half duplex.
- Auto-polarity detection and correction of incorrect polarity on the receive twisted-pair at each port.
- Data forwarding rate 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data forwarding rate 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- 12K active MAC address entry table per device with automatic learning and aging (10 to 1000000 seconds).
- 12 MB packet buffer per device.
- Broadcast storm filtering.
- IGMP Multicast support.
- 802.1Q VLANs.
- GARP/GVRP, GARP/GMRP support.
- DHCP Client.
- 802.1p Priority Queues.

Management

- RS-232 console port for out-of-band network management via a console terminal or PC.
- Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops.
- Fully configurable either in-band or out-of-band control via SNMP-based software.
- Flash memory for software upgrades. This can be done in-band via TFTP.
- Built-in SNMP management: Bridge MIB (RFC 1493), RMON MIB (RFC 1757), MIB-II (RFC 1213), Entity MIB version 2 (RFC 2737), and Proprietary MIBs.

2

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Switch.

Unpacking

Open the shipping carton of the Switch and carefully unpack its contents. The carton should contain the following items:

- One DES-3225G 24-port NWay Ethernet Switch
- One 2-port 100BASE-TX Fast Ethernet module preinstalled on front panel (DES-3225GF includes a 1-port 100BASE-FX module preinstalled).
- One console cable
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This User's Guide with Registration Card

If any item is found missing or damaged, please contact your local D-Link reseller for replacement.

Installation

Use the following guidelines when choosing a place to install the Switch:

- The surface must support at least 3 kg.
- The power outlet should be within 1.82 meters (6 feet) of the device.
- Visually inspect the power cord and see that it is secured to the AC power connector.
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch. Do not place heavy objects on the switch.

Desktop or Shelf Installation

When installing the Switch on a desktop or shelf, the rubber feet included with the device should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow adequate space for ventilation between the device and the objects around it.

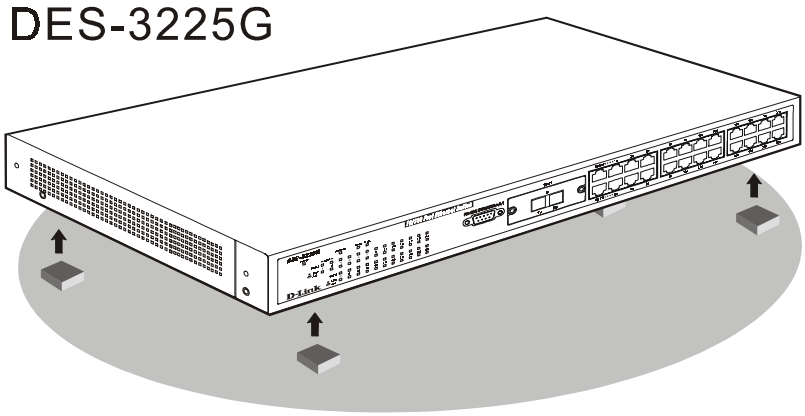


Figure 2-1. Installing rubber feet for desktop installation

Rack Installation

The DES-3225G can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.

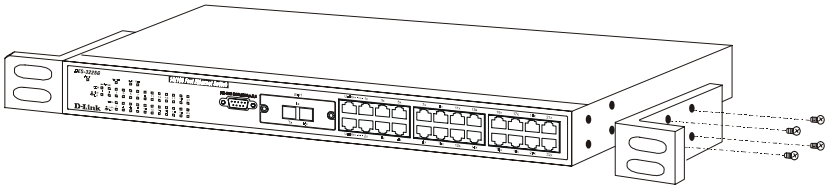


Figure 2- 2A. Attaching the mounting brackets to the switch

Then, use the screws provided with the equipment rack to mount the switch on the rack.

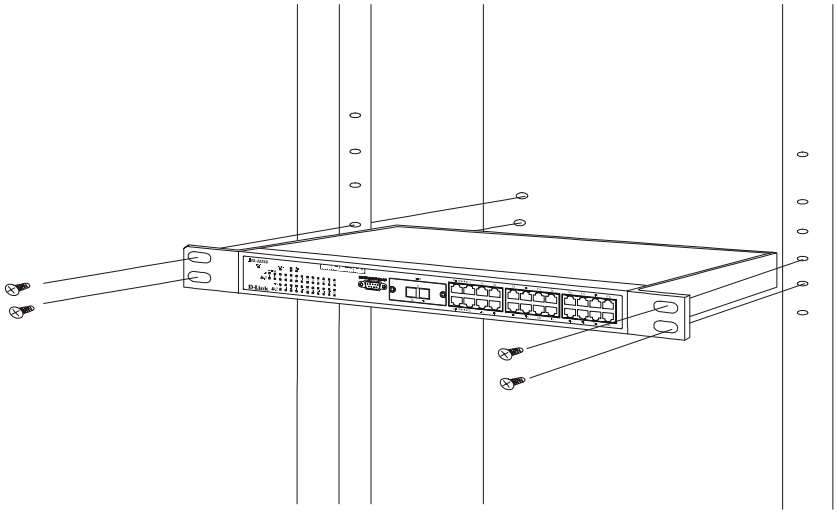


Figure 2-2B. Installing the switch on an equipment rack

Power on

The DES-3225G switch can be used with AC power supply 100 - 240 VAC, 50/60 Hz. The Switch's power supply will adjust to the local power source automatically and may be used without having any or all LAN segment cables connected.

After the switch is plugged in, the LED indicators should respond as follows:

- All LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.
- The power LED indicator will blink while the Switch loads onboard software and performs a self-test. After approximately 20 seconds, the LED will light again to indicate the switch is in a ready state.
- The console LED indicator will remain ON if there is a connection at the RS-232 port, otherwise this LED indicator is OFF.
- The 100M LED indicator may remain ON or OFF depending on the transmission speed.

Power Failure

As a precaution, in the event of a power failure, unplug the switch. When power is resumed, plug the switch back in.

3

IDENTIFYING EXTERNAL COMPONENTS

This chapter describes the front panel, rear panel, optional plug-in modules, and LED indicators of the DES-3225G.

Front Panel

The front panel of the Switch consists of LED indicators, an RS-232 communication port, a slide-in module slot, two uplink ports, and 22 (10/100 Mbps) Ethernet/Fast Ethernet ports.

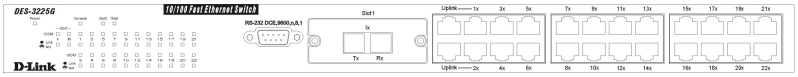


Figure 3-1. Front panel view of the Switch

- Comprehensive LED indicators display the status of the switch and the network. A description of these LED indicators follows (see the *LED Indicators* section below).
- An RS-232 DCE console port for setting up and managing the switch via a connection to a console terminal or PC using a terminal emulation program.
- A front-panel slide-in module slot for 10/100 Mbps Ethernet ports can accommodate a 2-port 10/100BASE-TX Fast Ethernet module, a 2-port 100BASE-FX MT-RJ type module, or a 1-port 100BASE-FX SC type module.
- Two MDI-II Uplink jacks which can be used to connect a straight-through cable to a normal (non-Uplink) port on a switch or hub. Do not use port 1X if the top Uplink port is occupied or Port 2X if the bottom Uplink port is occupied.
- Twenty-two high-performance, NWay Ethernet ports all of which operate at 10/100 Mbps for connections to end stations, servers and hubs. All ports can auto-negotiate between 10Mbps or 100Mbps, full- or half-duplex, and flow control.

Rear Panel

The rear panel of the switch consists of a slot for an optional Gigabit Ethernet fiber port and an AC power connector. The following displays the rear panel of the switch.

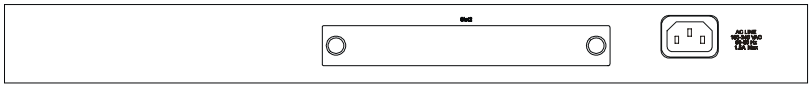


Figure 3-2. Rear panel view of the Switch

Figure 3-3. Rear panel view of the Switch fitted with the optional Gigabit Ethernet slide-in module

- The optional Gigabit Ethernet slide-in module (1000BASE-SX, 1000BASE-LX, or 1000BASE-T) contains one port for connecting to another switch.
- The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. Supported input voltages range from 100 ~ 240 VAC at 50 ~ 60 Hz.

Side Panels

The right side panel of the Switch contains two system fans (see the top part of the diagram below). The left side panel contains heat vents.

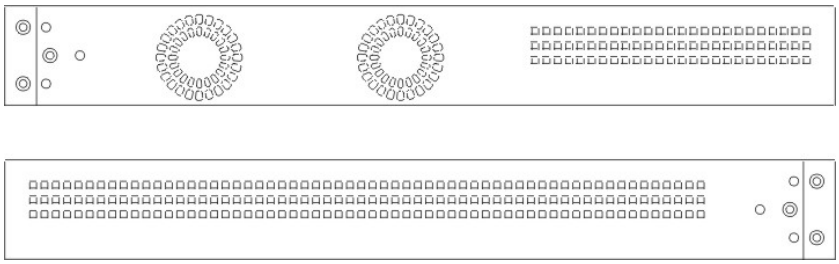


Figure 3-4. Side panel views of the Switch

- The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

Optional Plug-in Modules

The DES-3225G 24-port NWay Ethernet Switch is able to accommodate a range of plug-in modules in order to increase functionality and performance.

100BASE-TX Module

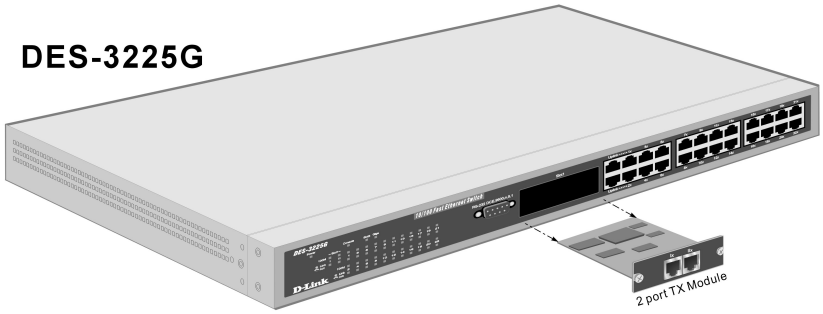


Figure 3-5. Two-port, 100BASE-TX module

- Two-port, front-panel module.
- Connects to 100BASE-TX devices at full- or half-duplex.
- Supports Category 5 UTP or STP cable connections of up to 100 meters.

100BASE-FX (SC) Fiber Module

Figure 3-6. One-port, 100BASE-FX (SC) module

- One-port, front-panel module.
- Connects to 100BASE-FX devices at full- or half-duplex.
- Supports multi-mode fiber-optic cable connections of up to 412 meters in half-duplex or 2 km in full-duplex mode.

100BASE-FX (MT-RJ) Fiber Module

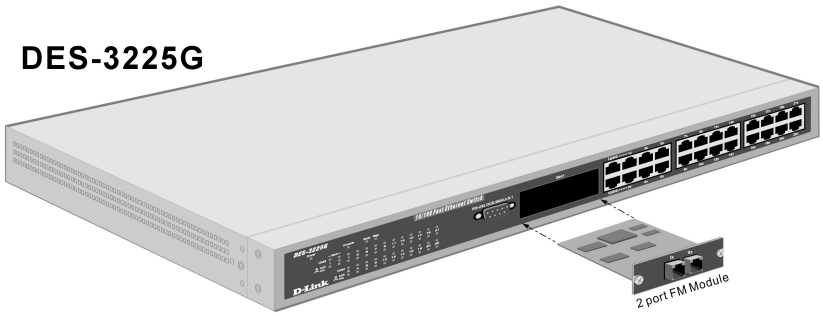


Figure 3-7. Two-port, 100BASE-FX (MT-RJ) module

- Two-port, front-panel module.
- Connects to 100BASE-FX devices at full- or half-duplex.
- Supports multi-mode fiber-optic cable connections of up to 412 meters in half duplex or 2 km in full duplex mode.

1000BASE-SX Gigabit Module

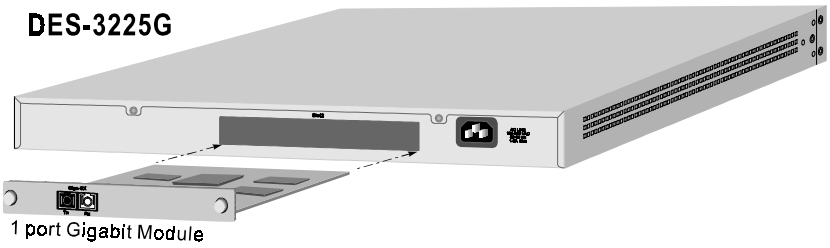


Figure 3-8. One-port, 1000BASE-SX module

- One-port, rear-panel module.
- Connects to 1000BASE-SX devices at full duplex or auto (auto negotiation is available in DES-3251G, version A3 and later).
- Allows connections using multi-mode fiber optic cable in the following configurations:

	62.5µm	62.5µm	50µm	50µm
Modal bandwidth (min. overfilled launch) Unit: MHz*km	160	200	400	500
Operating distance Unit: meters	220	275	500	550
Channel insertion loss Unit: dB	2.33	2.53	3.25	3.43

1000BASE-LX Gigabit Module

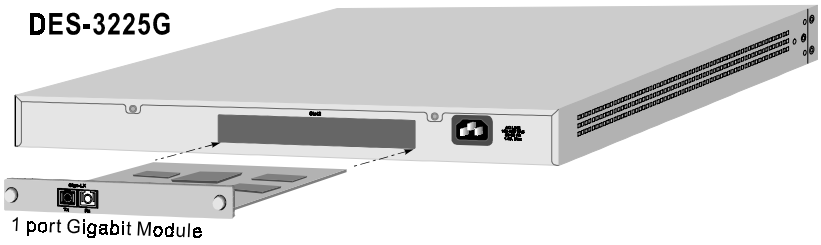


Figure 3-9. One-port, 1000BASE-LX module

- One-port, rear-panel module.

- Connects to 1000BASE-LX devices at full duplex or auto (auto negotiation is available in DES-3251GL, version A3 and later).
- Allows connections up to 5 km in length using single-mode fiber optic cable.

1000BASE-T Copper Gigabit Module

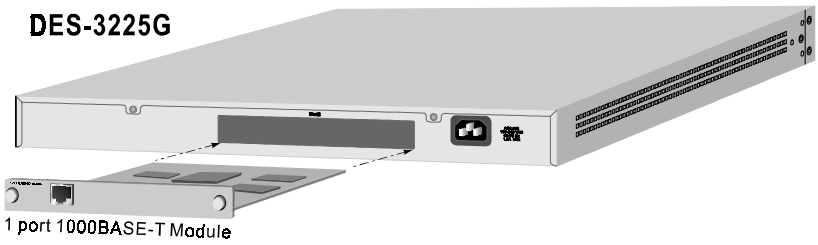


Figure 3-10. One-port, 1000BASE-T module

- One-port, rear-panel module.
- Connects to 1000BASE-T devices at 1000M/full duplex, 100M/full duplex, 100M/half duplex, and Auto.
- Supports Category 5+ or higher cable connections of up to 100 meters.

LED Indicators

The LED indicators of the Switch include Power, Console, Slot2, Giga, Speed, and Link/Act. The following shows the LED indicators for the Switch along with an explanation of each indicator.

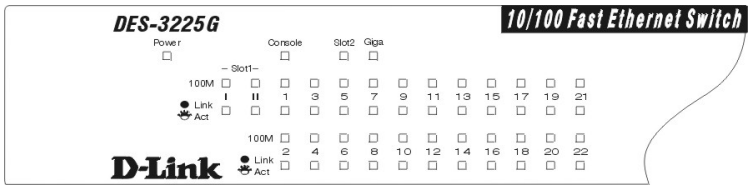


Figure 3-11. The LED indicators

- **Power** This indicator on the front panel should be colored amber during the Power-On Self Test (POST). It will light green approximately 2 seconds after the switch is powered on to indicate the ready state of the device. The LED will blink green while downloading new software for the switch, or if the system's configuration has changed and will light yellow when an error occurs.
- **Console** This indicator is lit green when the switch is being managed via out-of-band/local console management through the RS-232 console port using a straight-through serial cable.
- **Slot 2** This indicator is lit green when a Gigabit Ethernet slide-in module is present in the rear panel of the Switch.
- **Giga** This indicator is lit green when a link is established. It blinks green when the Gigabit port is active.
- **100M** These indicators are illuminated green when a 100 Mbps device is connected to any of the 24 ports or uplink port. If a 10 Mbps device is connected to any of the 24 ports or uplink port, these LEDs remain dark.

- **Link/Act** These indicators are lit when there is a secure connection (or link) to a device at any of the ports. The LEDs blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.

4

CONNECTING THE SWITCH

This chapter describes how to connect the DES-3225G to your Fast Ethernet network.

Switch to End Node

End nodes include PCs outfitted with a 10, 100 or 10/100 Mbps RJ-45 Ethernet/Fast Ethernet Network Interface Card (NIC) and most routers. The RJ-45 UTP ports on NICs and most routers are MDI-II. When using a normal straight-through cable, an MDI-II port must connect to an MDI-X port.

An end node can be connected to the Switch via a two-pair Category 3, 4, 5 UTP/STP straight cable (be sure to use Category 5 UTP or STP cabling for 100 Mbps Fast Ethernet connections). The end node should be connected to any of the twenty-two ports (1x - 22x) of the DES-3225G or to either of the two 100BASE-TX ports on the front-panel module that came preinstalled on the switch. An end node should not be connected to an Uplink port (unless using a crossover cable), and if the top Uplink port is in use, Port 1X must remain vacant; if the bottom Uplink port is in use, Port 2X cannot be used.

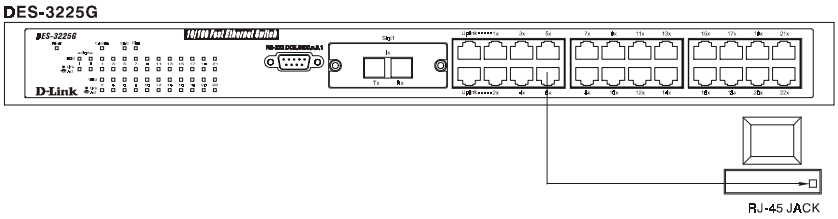


Figure 4-1. Switch connected to an End Node

The LED indicators for the port the end node is connected to are lit according to the capabilities of the NIC. If LED indicators are not illuminated after making a proper connection, check the PC's LAN card, the cable, switch conditions, and connections.

The following LED indicator states are possible for an end node to switch connection:

1. The 100M LED indicator comes *ON* for a 100 Mbps and stays *OFF* for 10 Mbps.

2. The Link/Act LED indicator lights up upon hooking up a PC that is powered on.

Switch to Hub or Switch

These connections can be accomplished in a number of ways. The most important consideration is that when using a normal, straight-through cable, the connection should be made between a normal crossed port (Port 1X, 2X, etc.) and an Uplink (MDI-II) port. If you are using a crossover cable, the connection must be made from Uplink to Uplink, or from a crossed port to another crossed port.

- A 10BASE-T hub or switch can be connected to the Switch via a two-pair Category 3, 4 or 5 UTP/STP straight cable.
- A 100BASE-TX hub or switch can be connected to the Switch via a two-pair Category 5 UTP/STP straight cable.

If the other switch or hub contains an unused Uplink port, we suggest connecting the other device's Uplink (MDI-II) port to any of the switch's (MDI-X) ports (1x - 22x, or one of the 100BASE-TX module ports) using a normal straight-through cable, as shown below.

If the other device does not have an unused Uplink port, make the connection with a normal straight-through cable from one of the Uplink ports on the switch to any normal crossed port on the hub. Alternatively, if you have a crossover cable you can save the Uplink ports for other connections and make this one from a crossed port to another crossed port.

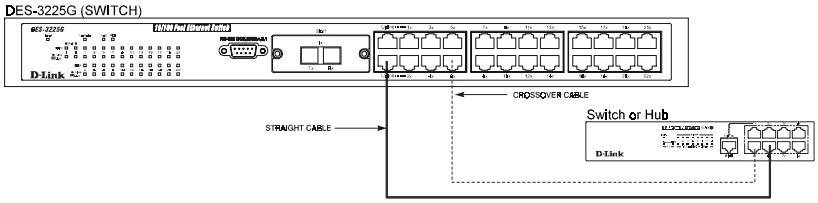


Figure 4-2. Switch connected to a normal (non-Uplink) port on a hub or switch using a straight or crossover cable

10BASE-T Device

For a 10BASE-T device, the Switch's LED indicators should display the following:

- 100M LED speed indicator is *OFF*.
- Link/Act indicator is *ON*.

100BASE-TX Device

For a 100BASE-TX device, the Switch's LED indicators should display the following:

- 100M LED speed indicator is *ON*.
- Link/Act is *ON*.

5

SWITCH MANAGEMENT CONCEPTS

This chapter discusses many of the features used to manage the switch, and explains many concepts and important points regarding these features. Configuring the switch to implement these concepts is discussed in detail in the next chapters.

Local Console Management

Local console management involves the administration of the DES-3225G Switch via a direct connection to the RS-232 DCE console port. This is an Out-Of-Band connection, meaning that it is on a different circuit than normal network communications, and thus works even when the network is down.

The local console management connection involves a terminal or PC running terminal emulation software to operate the switch's built-in console program (see Chapter 6, "*Using the Console Interface*"). Using the console program, a network administrator can manage, control and monitor the many functions of the Switch.

Hardware components in the Switch allow it to be an active part of a manageable network. These components include a CPU, memory for data storage, other related hardware, and SNMP agent firmware. Activities on the Switch can be monitored with these components, while the Switch can be manipulated to carry out specific tasks.

Diagnostic (console) port (RS-232 DCE)

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running terminal emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) a to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management done via management platforms, such as D-View, HP OpenView, etc.

The console port is set for the following configuration:

- ◊ Baud rate: 9,600
- ◊ Data width: 8 bits
- ◊ Parity: none
- ◊ Stop bits: 1
- ◊ Flow Control None

Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try hitting <Ctrl> + r to refresh the screen.

IP Addresses and SNMP Community Names

Each Switch has its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). You can change the default Switch IP Address to meet the specification of your networking address scheme.

In addition, you can also set an IP Address for a gateway router. This becomes necessary when the network management station is located on a different IP network as the Switch, making it necessary for management packets to go through a router to reach the network manager, and vice-versa.

For security, you can set in the Switch a list of IP Addresses of the network managers that you allow to manage the Switch. You can also change the default Community Name in the Switch and set access rights of these Community Names.

Traps

Traps are messages that alert you of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned *OFF* the Switch), or less serious like a port status change. The Switch generates traps and sends them to the network manager (trap managers). The following lists the types of events that can take place on the Switch.

- ◊ System resets
- ◊ Errors
- ◊ Status changes
- ◊ Topology changes
- ◊ Operation

You can also specify which network managers may receive traps from the Switch by setting a list of IP Addresses of the authorized network managers.

Trap managers are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap managers will receive traps sent from the Switch; they must immediately take certain actions to avoid future failure or breakdown of the network.

The following are trap types a trap manager will receive:

- **Cold Start** This trap signifies that the Switch has been powered up and initialized such that software settings are reconfigured and hardware systems are rebooted. A cold start is different from a factory reset.
- **Warm Start** This trap signifies that the Switch has been rebooted, however the POST (Power On Self-Test) is skipped.
- **Authentication Failure** This trap signifies that someone has tried to logon to the switch using an invalid SNMP community name. The switch automatically stores the source IP address of the unauthorized user.
- **New Root** This trap indicates that the Switch has become the new root of the Spanning Tree, the trap is sent by a bridge soon after its election as the new root. This implies that upon expiration of the

Topology Change Timer the new root trap is sent out immediately after the Switch's selection as a new root.

- **Topology Change** A Topology Change trap is sent by the Switch when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a new root trap is sent for the same transition.
- **Link Change Event** This trap is sent whenever the link of a port changes from link up to link down or from link down to link up.
- **Port Partition** This trap is sent whenever the port state enters the partition mode (or automatic partitioning, port disable) when more than thirty-two collisions occur while transmitting at 10Mbps or more than sixty-four collisions occur while transmitting at 100Mbps.
- **Broadcast Storm** This trap is sent whenever the port reaches the broadcast storm rising or falling threshold.
- **Address Table Full** This trap is sent whenever the MAC Address Table is full.
- **Entity MIB Change** This trap is sent whenever a MIB object of Entity MIB version 2 (RFC 2737) is changed.

MIBs

Management information and counters are stored in the Switch in the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network manager software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. These MIBs may also be retrieved by specifying the MIB's Object-Identity (OID) at the network manager. MIB values can be either read-only or read-write.

Read-only MIBs variables can be either constants that are programmed into the Switch, or variables that change while the Switch is in operation. Examples of read-only constants are the number of ports and types of ports. Examples of read-only variables are the statistics counters such as the number of errors that have occurred, or how many kilobytes of data have been received and forwarded through a port.

Read-write MIBs are variables usually related to user-customized configurations. Examples of these are the Switch's IP Address, Spanning Tree Algorithm parameters, and port status.

If you use a third-party vendors' SNMP software to manage the Switch, a diskette listing the Switch's propriety enterprise MIBs can be obtained by request. If your software provides functions to browse or modify MIBs, you can also get the MIB values and change them (if the MIBs' attributes permit the write operation). This process however can be quite involved, since you must know the MIB OIDs and retrieve them one by one.

Packet Forwarding

The Switch learns the network configuration and uses this information to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all segments, are transmitted to the destination only. Example: if Port 1 receives a packet destined for a station on Port 2, the Switch transmits that packet through Port 2 only, and transmits nothing through the other ports.

Aging Time

The Aging Time is a parameter that affects the auto-learn process of the Switch in terms of the network configuration. Dynamic Entries, which make up the auto-learned-node address, are aged out of the address table according to the Aging Time that you set.

The Aging Time can be from 10 seconds to 1000000 seconds. A very long Aging Time can result with the out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions.

In the opposite case, if the Aging Time is too short, many entries may be aged out soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Filtering Database

A switch uses a filtering database to segment the network and control communications between segments. It also filters packets off the network for intrusion control (MAC Address filtering).

For port filtering, each port on the switch is a unique collision domain and the switch filters (discards) packets whose destination lies on the same port as where it originated. This keeps local packets from disrupting communications on other parts of the network.

For intrusion control, whenever a switch encounters a packet originating from or destined to a MAC address defined by the user, the switch will discard the packet.

Filtering includes:

1. Dynamic filtering – automatic learning and aging of MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.
2. MAC address filtering – the manual entry of specific MAC addresses to be filtered from the network.
3. Filtering done by the Spanning Tree Protocol, which can filter packets based on topology, making sure that signal loops don't occur.
4. Filtering done for VLAN integrity. Packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3) will be filtered.

Spanning Tree Algorithm

The Spanning Tree Algorithm (STA) in the Switch allows you to create alternative paths (with multiple switches or other types of bridges) in your network. These backup paths are idle until the Switch determines that a problem has developed in the primary paths. When a primary path is lost, the switch providing the alternative path will automatically go into service with no operator intervention. This automatic network reconfiguration provides maximum uptime to network users. The concept of the Spanning Tree Algorithm is a complicated and complex subject and must be fully researched and understood. Please read the following before making any changes.

- **Network loop detection and prevention** With STA, there will be only one path between any two LANs. If there is more than one path, forwarded packets will loop indefinitely. STA detects any looped path and selects the path with the lowest path cost as the active path, while blocking the other path and using it as the backup path.

- **Automatic topology re-configuration** When the path for which there is a backup path fails, the backup path will be automatically activated, and STA will automatically re-configure the network topology.

STA Operation Levels

STA operates on two levels: the bridge level and the port level. On the bridge level, STA calculates the Bridge Identifier for each Switch, then sets the Root Bridge and the Designated Bridges. On the port level, STA sets the Root Port and Designated Ports. Details are as follows:

On the Bridge Level

- **Root Bridge** The switch with the lowest Bridge Identifier is the Root Bridge. Naturally, you will want the Root Bridge to be the best switch among the switches in the loop to ensure the highest network performance and reliability.
- **Bridge Identifier** This is the combination of the Bridge Priority (a parameter that you can set) and the MAC address of the switch. Example: 4 00 80 C8 00 01 00, where 4 is the Bridge Priority. A lower Bridge Identifier results in a higher priority for the switch, and thus increases it probably of being selected as the Root Bridge.
- **Designated Bridge** From each LAN segment, the attached Bridge that has the lowest Root Path Cost to the Root Bridge is the Designated Bridge. It forwards data packets for that LAN segment. In cases where all Switches have the same Root Path Cost, the switch with the lowest Bridge Identifier becomes the Designated Bridge.
- **Root Path Cost** The Root Path Cost of a switch is the sum of the Path Cost of the Root Port and the Root Path Costs of all the switches that the packet goes through. The Root Path Cost of the Root Bridge is zero.
- **Bridge Priority** This is a parameter that users can set. The smaller the number you set, the higher the Bridge Priority is. The higher the Bridge Priority, the better the chance the Switch will be selected as the Root Bridge.

On the Port Level

- **Root Port** Each switch has a Root Port. This is the port that has the lowest Path Cost to the Root Bridge. In case there are several such ports, then the one with the lowest Port Identifier is the Root Port.
- **Designated Port** This is the port on each Designated Bridge that is attached to the LAN segment for which the switch is the Designated Bridge.
- **Port Priority** The smaller this number, the higher the Port Priority is. With higher Port Priority, the higher the probability that the port will be selected as the Root Port.
- **Path Cost** This is a changeable parameter and may be modified according to STA specifications. Each 10Mbps and 100Mbps segment has an assigned Path Cost of 19.

User-Changeable STA Parameters

The factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

- **Bridge Priority** A Bridge Priority can be from 0 to 65535. 0 is equal to the highest Bridge Priority.
- **Bridge Hello Time** The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

  Note: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.
- **Bridge Max. Age** The Max. Age can be from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.
- **Bridge Forward Delay** The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

  Observe the following formulas when you set the above parameters:

  1. Max. Age ≤ 2 x (Forward Delay - 1 second)
  2. Max. Age ≥ 2 x (Hello Time + 1 second)
- **Port Priority** A Port Priority can be from 0 to 255. The lower the number, the greater the probability the port will be chosen as the Root Port.

Illustration of STA

A simple illustration of three Bridges (or the Switch) connected in a loop is depicted in *Figure 5-1*. In this example, you can anticipate some major network problems if the STA assistance is not applied. For instance, if Bridge 1 broadcasts a packet to Bridge 2, Bridge 2 will broadcast it to Bridge 3, and Bridge 3 will broadcast it to Bridge 1...and so on. The broadcast packet will be passed indefinitely in a loop, causing a serious network failure.

To alleviate network loop problems, STA can be applied as shown in *Figure* 5-2. In this example, STA breaks the loop by blocking the connection between Bridge 1 and 2. The decision to block a particular connection is based on the STA calculation of the most current Bridge and Port settings. Now, if Bridge 1 broadcasts a packet to Bridge 3, then Bridge 3 will broadcast it to Bridge 2 and the broadcast will end there.

STA setup can be somewhat complex. Therefore, you are advised to keep the default factory settings and STA will automatically assign root bridges/ports and block loop connections. However, if you need to customize the STA parameters, refer to *Table 5-1*.

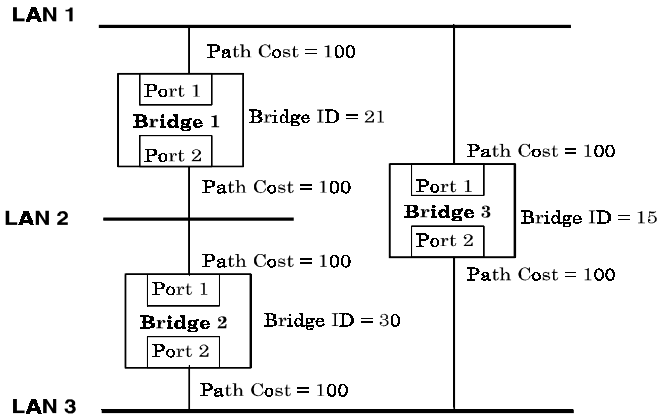


Figure 5-1. Before Applying the STA Rules

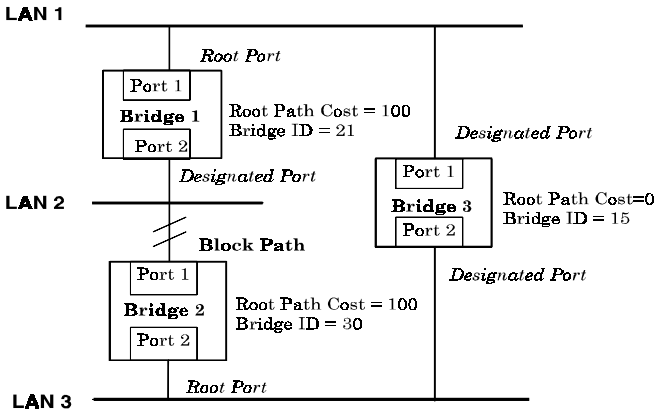


Figure 5-2. After Applying the STA Rules

STA parameters	Settings	Effects	Comment
Bridge Priority	lower the #, higher the priority	Increases chance of becoming the Root Bridge	Avoid, if the switch is used in workgroup level of a large network
Hello Time	1 - 10 sec.	No effect, if not Root Bridge	Never set greater than Max. Age Time
Max. Age Time	6 - 40 sec.	Compete for Root Bridge, if BPDU is not received	Avoid low number for unnecessary reset of Root Bridge
Forward Delay	4 - 30 sec.	High # delays the change in state	Max. Age ≤ 2 x (Forward Delay - 1) Max. Age ≥ 2 x (Hello Time + 1)
Port Level STA parameters			
Enable / Disable	Enable / Disable	Enable or disable this LAN segment	Disable a port for security or problem isolation
Port Priority	lower the #, higher the priority	Increases chance of become Root Port	

Table 5-1. User-selective STA parameters

Port Trunking

Port trunking is used to combine a number of ports together to make a single high-bandwidth data pipeline. The participating parts are called members of a trunk group, with one port designated as the *master* of the group. Since all members of the trunk group must be configured to operate in the same manner, all settings

changes made to the master port are applied to all members of the trunk group. Thus, when configuring the ports in a trunk group, you only need to configure the master port.

The DES-3225G supports 3 trunk groups, which may include from 2 to 8 switch ports each, except for the third trunk group which consists of the 2 ports of the Slot 1, 100BASE-TX or 100BASE-FX front-panel module. The master port for the first group is preset as port 7, the master port for the second group is port 15 and the master port for the third group is the first port (1x) on the 2-port module.

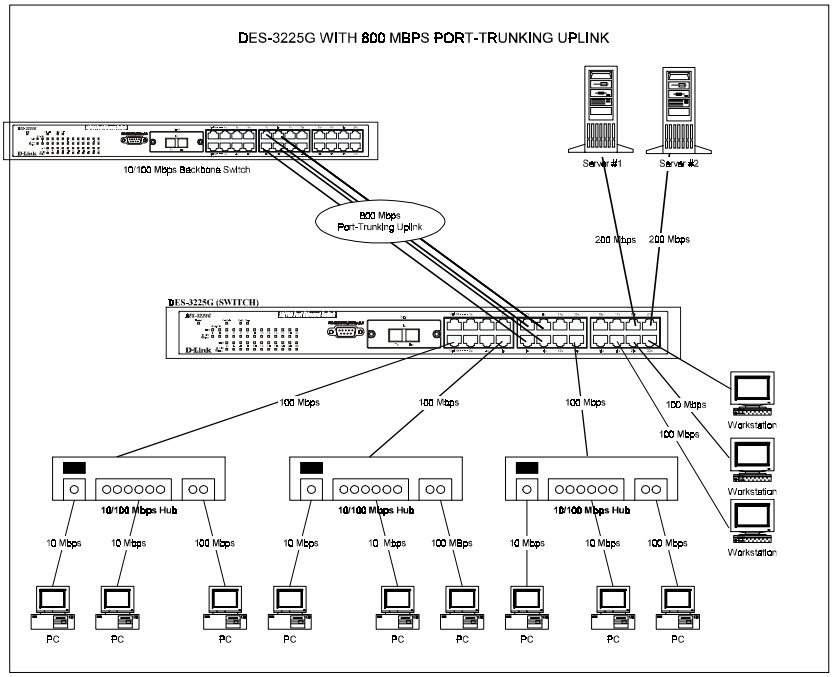


Figure 5-3. Port trunking example

The switch treats all ports in a trunk group as a single port. As such, trunk ports will not be blocked by Spanning Tree.

Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent. A trunk connection can be made with any other switch that maintains host-to-host data streams over a single trunk port. Switches that use a load-balancing scheme that sends the packets of a host-to-host data stream over multiple trunk ports cannot have a trunk connection with the DES-3225G switch.

VLANs and Broadcast Domains

VLANs are a collection of users or switch ports grouped together in a secure, autonomous broadcast and multicast domain. The main purpose of setting up VLANs or a broadcast domain on a network is to limit the range and effects of broadcast packets.

Two types of VLANs are implemented on the Switch: 802.1Q VLANs and port-based VLANs. MAC-based broadcast domains are a third option. Only one type of VLAN or broadcast domain can be active on the Switch at any given time, however. Thus, you will need to choose the type of VLAN or broadcast domain you wish to setup on your network and configure the Switch accordingly. 802.1Q VLANs support IEEE 802.1Q tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant). In contrast, MAC-based broadcast domains are limited to the Switch and devices directly connected to them.

All VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All broadcast, multicast, and unknown packets entering the Switch on a particular VLAN will only be forwarded to the stations or ports (802.1Q and port-based) that are members of that VLAN. 802.1Q and port-based VLANs also limit unicast packets to members of the VLAN, thus providing a degree of security to your network.

Another benefit of 802.1Q and port-based VLANs is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN (the sales VLAN, for example) to another VLAN (the marketing VLAN). This allows VLANs to accommodate network moves, changes and additions with the utmost flexibility. MAC-based broadcast domains, on the other hand, allow a station to be physically moved yet still belong to the same broadcast domain without having to change and configuration settings.

The *untagging* feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The *tagging* feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally (BPDU packets are not tagged).

MAC-based Broadcast Domains

The Switch supports up to 12 MAC-based broadcast domains, which are by their nature, limited to the Switch itself and the devices connected directly to it.

Since MAC addresses are hard-wired into a station's network interface card (NIC), MAC-based broadcast domains enable network managers to move a station to a different physical location on the network and have that station automatically retain its broadcast domain membership. This provides the network with a high degree of flexibility since even notebook PC's can plug into any available port on a network and communicate with the same people and use the same resources that have been allocated to the broadcast domain in which it is a member.

Since MAC-based broadcast domains do not restrict the transmission of known unicast frames to other broadcast domains, they can only be used to define limited broadcast domains. As such, they are best implemented on networks where stations are frequently moving, for example where people using notebook PCs are constantly plugging into different parts of the network.

Setting up MAC-based broadcast domains is a relatively straightforward process. Simply create the broadcast domain by assigning it a name (description) and add MAC addresses for the stations that will be members.

802.1Q VLANs

The Switch supports up to 4094 802.1Q VLANs. 802.1Q VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On 802.1Q VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another Switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

There are two key components to understanding 802.1Q VLANs: Port VLAN ID numbers (PVIDs) and VLAN ID numbers (VIDs). Both variables are assigned to a switch port, but there are important differences between them. A user can only assign one PVID to each switch port. The PVID defines which VLAN a packet belongs to when packets need to be forwarded to another switch port or somewhere else on the network. On the other hand, a user can define a port as a member of multiple VLANs (VIDs), allowing the segment connected to it to receive packets from many VLANs on the network. These two variables control a port's ability to transmit and

receive VLAN traffic, and the difference between them provides network segmentation, while still allowing resources to be shared across more than one VLAN.

802.1Q VLAN Segmentation

The following example is helpful in explaining how 802.1Q VLAN segmentation works. Take a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2 and has the Port VLAN ID number 2 (PVID=2). If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2, because it's Port VLAN ID number is 2 (PVID=2).

Sharing Resources Across 802.1Q VLANs

Network resources such as printers and servers however, can be shared across 802.1Q VLANs. This is achieved by setting up overlapping VLANs as shown in the diagram below.

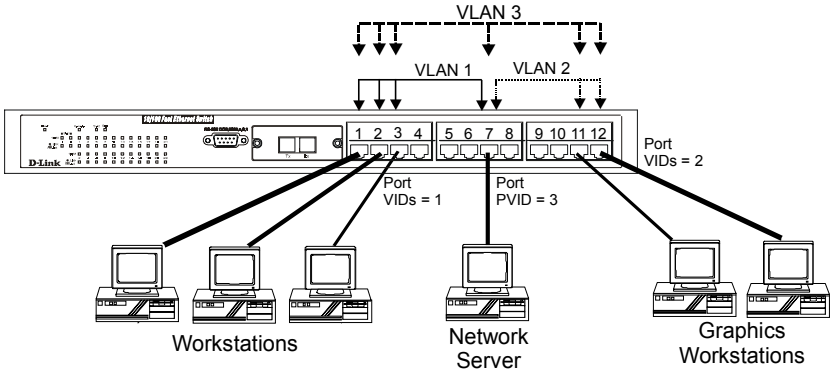


Figure 5-4. Example of typical VLAN configuration

In the above example, there are three different 802.1Q VLANs and each port can transmit packets on one of them according to their Port VLAN ID (PVID). However, a port can receive packets on all VLANs (VID) that it belongs to. The assignments are as follows:

PVID (Port VLAN ID)	*Ports*
1	Port 1
1	Port 2
1	Port 3
2	Port 11
2	Port 12
3	Port 7

VID (VLAN ID)	*Member Ports*
1	1,2,3,7
2	7,11,12
3	1,2,3,7,11,12

Table 5-2. VLAN assignments for Figure 5-4

The server attached to Port 7 is shared by VLAN 1 and VLAN 2 because Port 7 is a member of both VLANs (it is listed as a member of VID 1 and 2). Since it can receive packets from both VLANs, all ports can successfully

send packets to it. Ports 1, 2 and 3 send these packets on VLAN 1 (their PVID=1), and Ports 11 and 12 send these packets on VLAN 2 (PVID=2). The third VLAN (PVID=3) is used by the server to transmit files that had been requested on VLAN 1 or 2 back to the computers. All computers that use the server will receive transmissions from it since they are all located on ports which are members of VLAN 3 (VID=3).

802.1Q VLANs Spanning Multiple Switches

802.1Q VLANs can span multiple switches as well as your entire network. Two considerations to keep in mind while building VLANs of this sort are whether the switches are IEEE 802.1Q-compliant and whether VLAN packets should be tagged or untagged.

Definitions of relevant terms are as follows:

- **Tagging** The act of putting 802.1Q VLAN information into the header of a packet. Tagging ports will put the VID number, priority, and other VLAN information into all packets that flow out it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Tagging is used to send packets from one 802.1Q-compliant device to another.

- **Untagging** The act of stripping 802.1Q VLAN information out of the packet header. Untagging ports will take all VLAN information out of all packets that flow out of a port. If the packet doesn't have a VLAN tag, the port will not alter the packet, thus keeping the packet free of VLAN information. Untagging is used to send packets from an 802.1Q-compliant switch to a non-compliant device.

- **Ingress port** A port on a switch where packets are flowing into the switch. If an ingress port has the Ingress Filter enabled, the switch will examine each packet to determine whether or not it is a VLAN member and then take one of two actions: if the port is not a member of a VLAN, the packet will be dropped; if the port is a member of a VLAN, then the packet will be forwarded. Otherwise, if the Ingress Filter is disabled, then the switch will process any packet received at this port in its normal fashion.

- **Egress port** A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made. If an egress port is connected to an 802.1Q-compliant device, tagging should be enabled so the other device can take VLAN data into account when making forwarding decisions (this allows VLANs to span multiple switches). If an egress connection is to a non-compliant switch or end-station, tags should be stripped so the (now normal Ethernet) packet can be read by the receiving device.

VLANs Over 802.1Q-compliant Switches

When switches maintaining the same VLANs are 802.1Q-compliant, it is possible to use tagging. Tagging puts 802.1Q VLAN information into each packet header, enabling other 802.1Q-compliant switches that receive the packet to know how to treat it. Upon receiving a tagged packet, an 802.1Q-compliant switch can use the information in the packet header to maintain the integrity of VLANs, carry out priority forwarding, etc.

Data transmissions between 802.1Q-compliant switches take place as shown below.

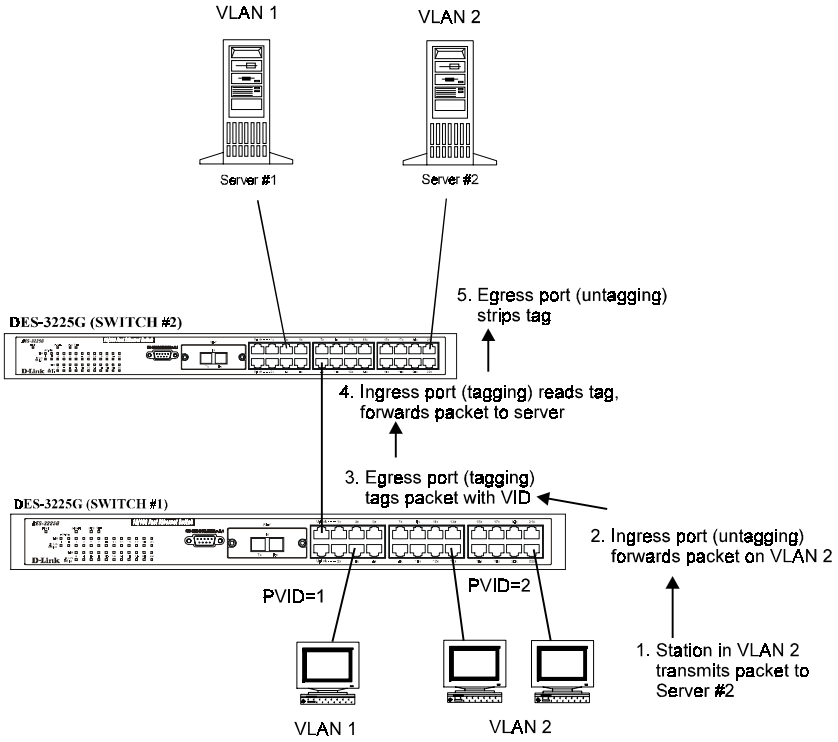

VLAN 1
VLAN 2
Server #1
Server #2
5. Egress port (untagging) strips tag
DES-3225G (SWITCH #2)
4. Ingress port (tagging) reads tag, forwards packet to server
3. Egress port (tagging) tags packet with VID
DES-3225G (SWITCH #1)
2. Ingress port (untagging) forwards packet on VLAN 2
PVID=1
PVID=2
1. Station in VLAN 2 transmits packet to Server #2
VLAN 1
VLAN 2

Figure 5-5. Data transmissions between 802.1Q-compliant Switches

In the above example, step 4 is the key element. Because the packet has 802.1Q VLAN data encoded in its header, the ingress port can make VLAN-based decisions about its delivery: whether server #2 is attached to a port that is a member of VLAN 2 and thus, should the packet be delivered; the queuing priority to give to the packet, etc. It can also perform these functions for VLAN 1 packets as well, and, in fact, for any tagged packet it receives regardless of the VLAN number.

If the ingress port in step 4 were connected to a non-802.1Q-compliant device and was thus receiving untagged packets, it would tag its own PVID onto the packet and use this information to make forwarding decisions. As a result, the packets coming from the non-compliant device would automatically be placed on the ingress ports VLAN and could only communicate with other ports that are members of this VLAN.

Port-based VLANs

Port-based VLANs are a simplified version of the 802.1Q VLANs described in the previous section. In port-based VLANs, all the 802.1Q settings are pre-configured allowing you to quickly and easily setup and maintain port-based VLANs on your network.

In port-based VLANs, broadcast, multicast and unknown packets will be limited to within the VLAN. Thus, port-based VLANs effectively segment your network into broadcast domains. Furthermore, ports can only belong to a single VLAN.

Because port-based VLANs are uncomplicated and fairly rigid in their implementation, they are best used for network administrators who wish to quickly and easily setup VLANs in order to isolate limit the effect of broadcast packets on their network.

For the most secure implementation, make sure that end stations are directly connected to the switch. Attaching a hub, switch or other repeater to the port causes all stations attached to the repeater to become members of the Port-based VLAN.

To setup port-based VLANs, simply select one of 24 VLAN ID numbers, name the VLAN and specify which ports will be members. All other ports will automatically be forbidden membership, even dynamically as a port can belong to only one VLAN.

Broadcast Storms

Broadcast storms are a common problem on today's networks. Basically, they consist of broadcast packets that flood and/or are looped on a network causing noticeable performance degradation and, in extreme cases, network failure. Broadcast storms can be caused by network loops, malfunctioning NICs, bad cable connections, and applications or protocols that generate broadcast traffic, among others.

In effect, broadcast storms can originate from any number of sources, and once they are started, they can be self-perpetuating, and can even multiply the number of broadcast packets on the network over time. In the best case, network utilization will be high and bandwidth limited until the hop counts for all broadcast packets have expired, whereupon the packets will be discarded and the network will return to normal. In the worst case, they will multiply, eventually using up all the network bandwidth (although network applications will usually crash long before this happens), and cause a network meltdown.

Broadcast storms have long been a concern for network administrators with routers traditionally being used to prevent their occurrence, and if that failed, to at least limit their scope. However, with the advent of VLANs, switches are now able to limit broadcast domains better and cheaper than routers. Also, many switches, including the DES-3225G series, have broadcast sensors and filters built into each port to further control broadcast storms.

Segmenting Broadcast Domains

The Switch allows you to segment broadcast domains. It does this by forwarding packets only to ports in the same broadcast domain or VLAN. Thus, broadcast packets will only be forwarded to ports that are members of the same broadcast domain or VLAN. Other parts of the network are effectively shielded. As a result, the smaller the broadcast domain, the less effect a broadcast storm will have. Since VLANs and broadcast domains are implemented at each switch port, they can be quite effective in limiting the scope of broadcast storms.

Eliminating Broadcast Storms

SNMP agents can be programmed to monitor the number of broadcast packets on switch ports and act on the data. When the number of broadcast packets on a given port rise past an assigned threshold, an action can be triggered. When enabled, the usual action is to block the port to broadcast frames, which discards all broadcast frames arriving at the port from the attached segment. Not only does this isolate the broadcast domain, but it actually starts removing broadcast packets from the affected segment. When the number of broadcast packets falls to an acceptable level (below a *falling threshold*), the SNMP agent can remove the blocking condition, returning the port to its normal operational state.

In the Switch, the default rising threshold is met when more than 500 broadcast packets per second are being detected on a specified port. Once the rising threshold is surpassed for a duration of more than 5 seconds, it will trigger the broadcast storm rising action configured by the user. The default falling threshold is met if there are less than 250 broadcast packets per second. It is triggered once the duration is at least 30 seconds. The actions can easily be defined by using a normal SNMP management program or through the console interface.

6

USING THE CONSOLE INTERFACE

Your 24-port NWay Ethernet Switch supports a console management interface that allows you to set up and control your Switch, either with an ordinary terminal (or terminal emulator), or over the network using the TCP/IP Telnet protocol. You can use this facility to perform many basic network management functions. In addition, the console program will allow you to set up the Switch for management using an SNMP-based network management system. This chapter describes how to use the console interface to access the Switch, change its settings, and monitor its operation.

Setting Up A Console

First-time configuration must be carried out through a "console," that is, either (a) a VT100-type serial data terminal, or (b) a computer running communications software set to emulate a VT100. The console must be connected to the Diagnostics port. This is an RS-232 port with a 9-socket D-shell connector and DCE-type wiring. Make the connection as follows:

1. Obtain suitable cabling for the connection.

   You can use either (a) a "null-modem" RS-232 cable or (b) an ordinary RS-232 cable and a null-modem adapter. One end of the cable (or cable/adapter combination) must have a 9-pin D-shell connector suitable for the Diagnostics port; the other end must have a connector suitable for the console's serial communications port.

2. Power down the devices, attach the cable (or cable/adapter combination) to the correct ports, and restore power.

3. Set the console to use the following communication parameters for your terminal:

- 9600 baud
- No parity checking (sometimes referred to as "no parity")
- 8 data bits (sometimes called a "word length" of 8 bits)
- 1 stop bit (sometimes referred to as a 1-bit stop interval)
- VT-100/ANSI compatible
- Arrow keys enabled

A typical console connection is illustrated below:

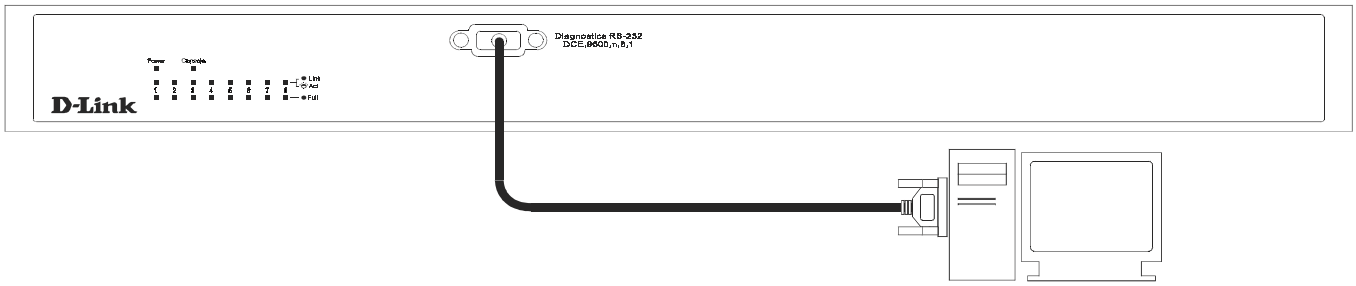


Figure 6-1. Example of a console connection

Connecting to the Switch Using Telnet

Once you have set an IP address for your Switch, you can use a Telnet program (in a VT-100 compatible terminal mode) to access and control the Switch. Most of the screens are identical, whether accessed from the console port or from a Telnet interface. You can also use a Web-based browser to manage the Switch. See the next chapter, *"Web-Based Network Management,"* for further information.

Console Usage Conventions

The console interface makes use of the following conventions:

1. Items in **<***angle brackets***>** can be toggled on or off using the space bar.
2. Items in **[***square brackets***]** can be changed by typing in a new value. You can use the backspace and delete keys to erase characters behind and in front of the cursor.
3. The up and down arrow keys, the left and right arrow keys, the tab key and the backspace key, can be used to move between selected items. It is recommended that you use the tab key and backspace key for moving around console.
4. Items in UPPERCASE are commands. Moving the selection to a command and pressing Enter will execute that command, e.g. APPLY, etc.

Please note that the command APPLY only applies for the current session. Use **Save Changes** from the main menu for permanent changes. An asterisk "*" indicates a change has been made but won't take effect until the Switch has been rebooted.

First Time Connecting To The Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch.

Note: The passwords used to access the Switch are case sensitive; therefore, "S" is not the same as "s."

When you first connect to the Switch, you will be presented with the first login screen (shown below). Press Ctrl+R (hold down the Ctrl key, press the R key, and release both keys) to call up the screen, if the initial login screen does not appear. Also Ctrl+R can be used at any time to refresh the screen.

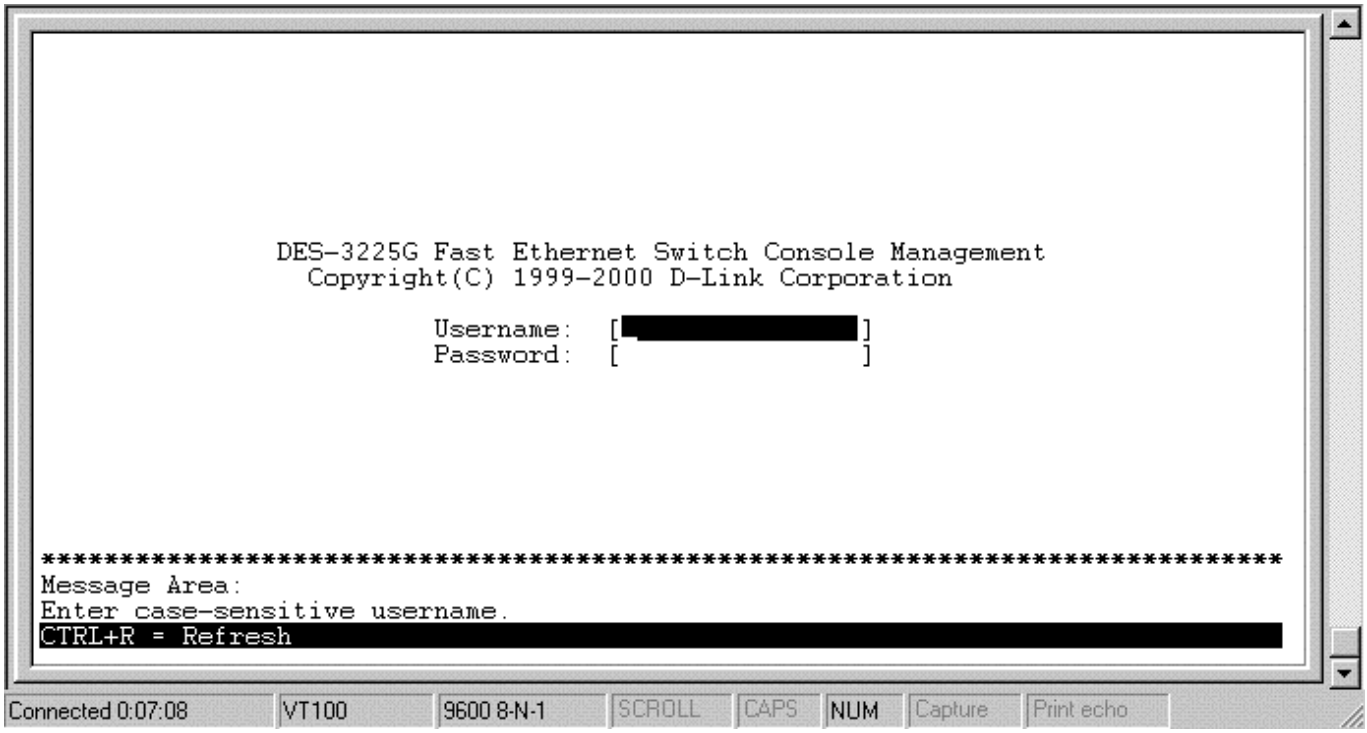


Figure 6-2. Initial screen, first time connecting to the Switch

Note: There is no initial username or password. Leave the Username and Password fields blank.

Press <Enter> or <Return> in the Username and Password fields. You will be given access to the main menu shown below:

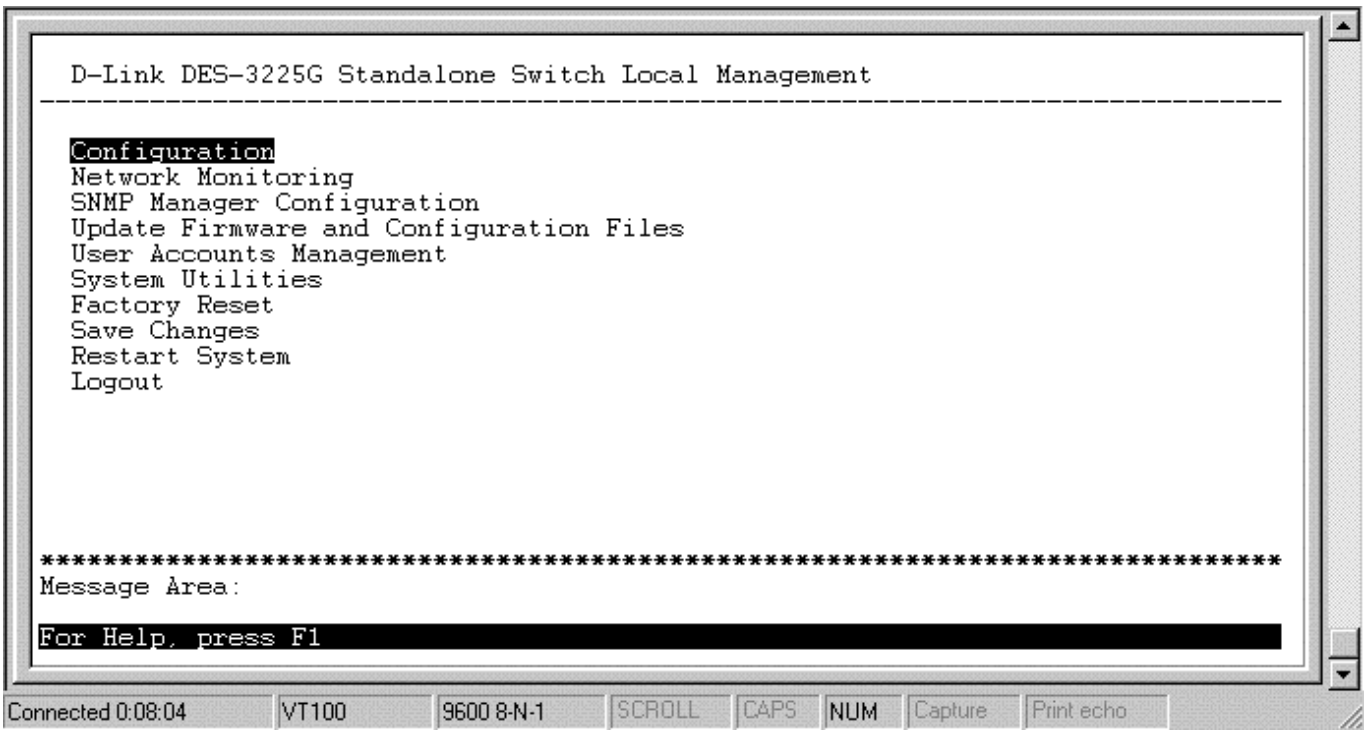


Figure 6-3. Main menu

The first user automatically gets Administrator privileges (See *Table 6-1*). It is recommended to create at least one Administrator-level user for the Switch.

User Accounts Management

From the screen above, move the cursor to the **User Accounts Management** menu and press <Enter>, then the **Users Accounts Management** menu appears.

1. Choose **Create/Modify User Accounts** from the **User Accounts Management** menu and the **Add/Modify User Accounts** menu appears.

2. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have Administrator or Normal User privileges. (Use the space bar to toggle between the two options).

3. Press APPLY to let the user addition take effect.

4. Press <Esc> to return to the previous screen or Ctrl+T to go to the root screen.

5. To see a listing of all user accounts and access levels, press <Esc>. Then choose **View/Delete User Accounts**. The **View/Delete User Accounts** screen appears.

Administrator and Normal User Privileges

There are two levels of user privileges: *Administrator* and *Normal User*. Some menu selections available to users with *Administrator* privileges may not be available to *Normal User*s. The main menus shown are the menus for the two types of users:

The following table summarizes Administrator and Normal User privileges:

Menu	Administrator	Normal User
	Privilege	
Configuration	Yes	Yes, view only.
Network Monitoring	Yes	Yes, view only.
Community Strings and Trap Stations	Yes	Yes, view only.
Update Firmware and Configuration Files	Yes	No
User Accounts Management		
Create/Modify User Accounts	Yes	No
View/ Delete User Accounts	Yes	No
System Utilities	Yes	Yes
Factory Reset	Yes	No
Restart System	Yes	No

Table 6-1. Administrator and Normal User Privileges

After establishing a User Account with **Administrator**-level privileges, press <Esc> twice. Then choose the **Save Changes** menu (see below). Pressing any key will return to the main menu. You are now ready to operate the Switch.

Saving Changes

The DES-3225G has two levels of memory normal RAM and non-volatile or NV-RAM. Settings need to be changed in all screens by clicking on the Apply button. When this is done, the settings will be immediately

applied to the switching software in RAM, and will immediately take effect. Some settings, though, require you to restart the switch before they will take effect. Restarting the switch will erase all settings in RAM and reload them from the NV-RAM. Thus, it is necessary to save all settings to the NV-RAM before restarting the switch.

In order to retain any modifications made in the current session by saving them into the NV-RAM, it is necessary to choose **Save Changes** from the main menu. The following screen will appear to indicate your new settings have been processed:

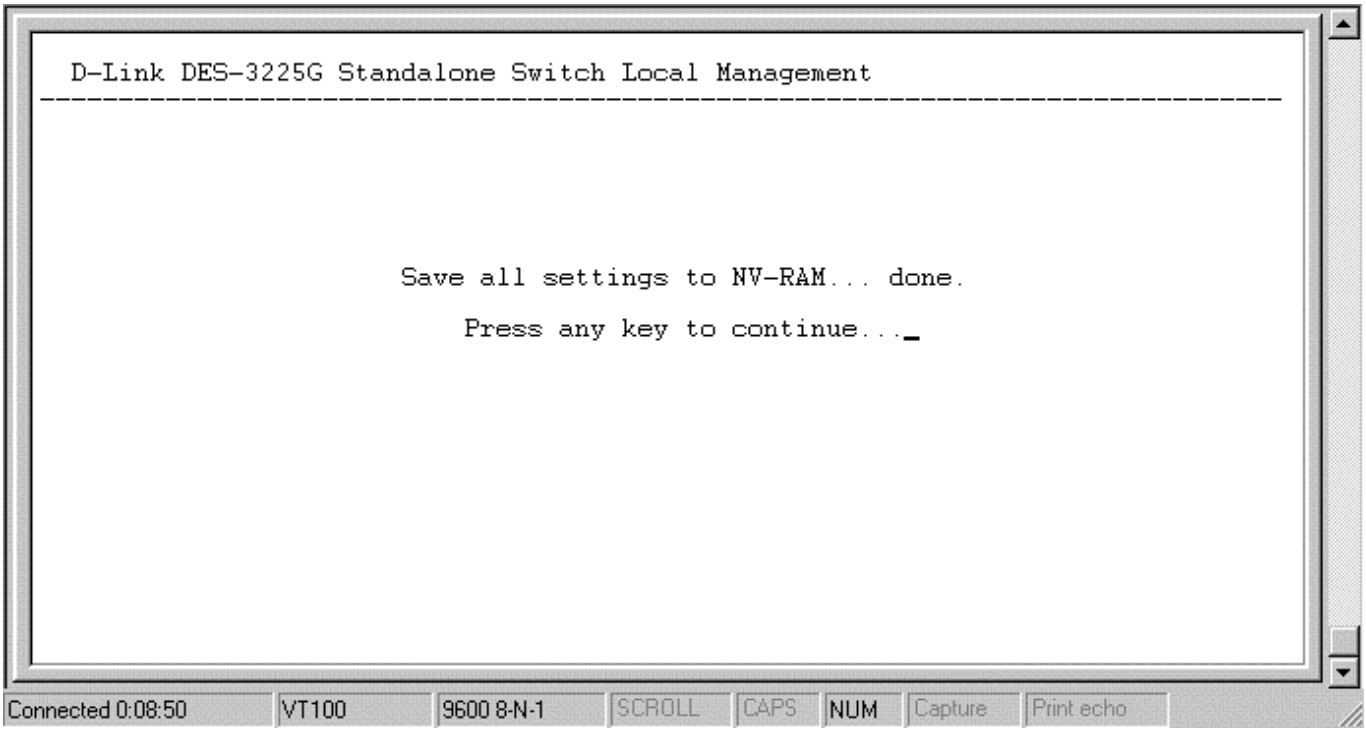


Figure 6-4. Save Changes screen

After the settings have been saved to NV-RAM, they will become the default settings for the switch, and they will be used by the switch every time it is powered on, reset or rebooted. The only exception to this is a factory reset, which will clear all settings and restore them to their initial values listed in *Appendix D*, which were present when the switch was purchased.

Logging Onto The Switch Console By Registered Users

To log in once you have created a registered user,

1. Type in your Username and press <Enter>.
2. Type in your Password and press <Enter>.
3. The main menu screen will be displayed based on your *Administrator* or *Normal User* access level or privilege.

Create/Modify User Accounts

To add or change your user password:

Choose **Users Accounts Management** from the main menu. The following **User Accounts Management** menu appears:

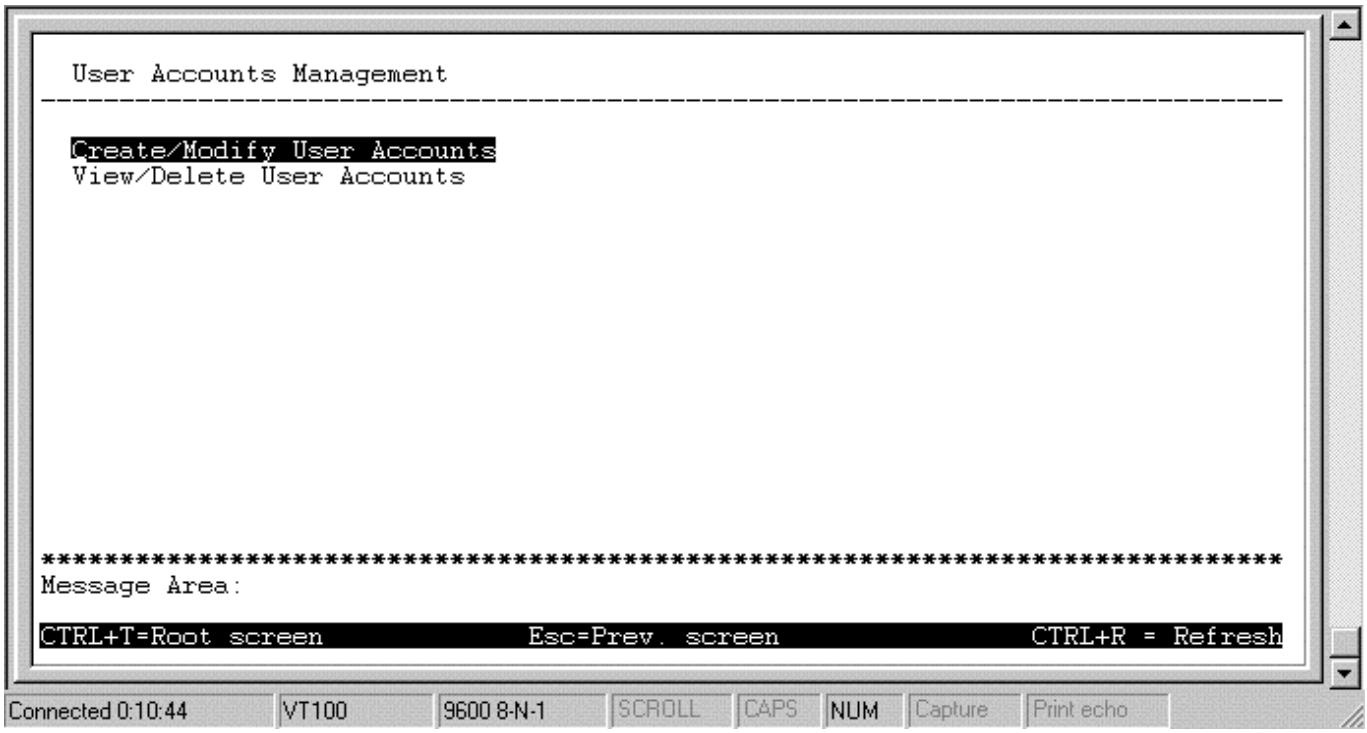


Figure 6-5. User Accounts Management menu

1. Choose **Create/Modify User Accounts**. The following screen appears:

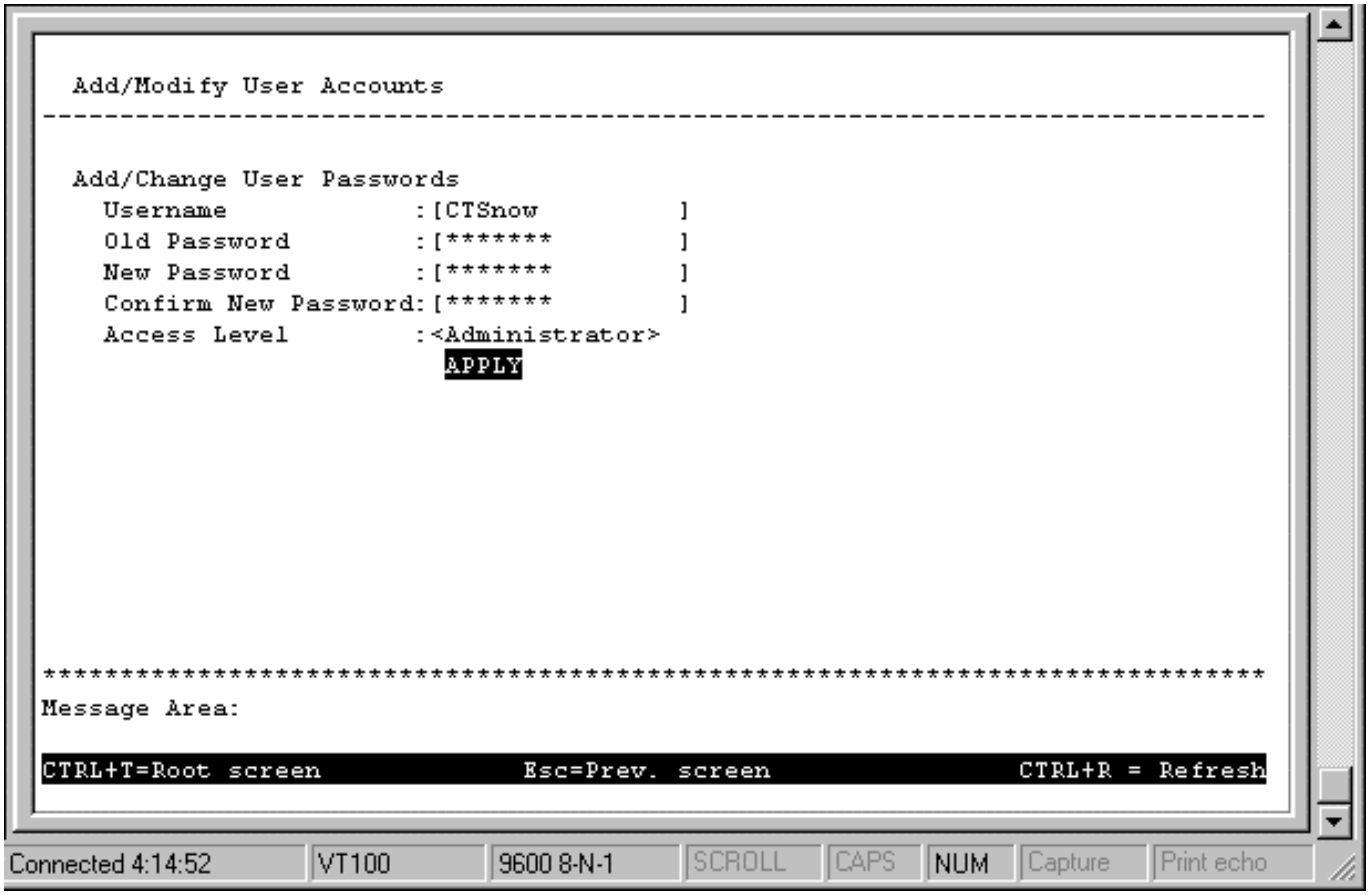


Figure 6-6. Add/Modify User Accounts screen

2. Type in your Username and press <Enter>.

3. If you are a new user, type in the Old Password and press <Enter>.

4. Type in the New Password you have chosen, and press <Enter>. Type in the same new password in the following field to verify that you have not mistyped it.

5. Determine whether the new user should have *Normal User* or *Administrator* privileges.

6. Choose the APPLY command to let the password change take effect.

This method can also be used by an *Administrator*-level user to change another user's password.

View/Delete User Accounts

Access to the console, whether using the console port or via Telnet, is controlled using a user name and password. Up to three of these user names can be defined. The console interface will not let you delete the current logged-in user, however, in order to prevent accidentally deleting all of the users with *Administrator* privilege.

Only users with the *Administrator* privilege can delete users.

To view your user password:

Choose **View/Delete User Accounts** from the **User Accounts Management** menu. The following screen appears:

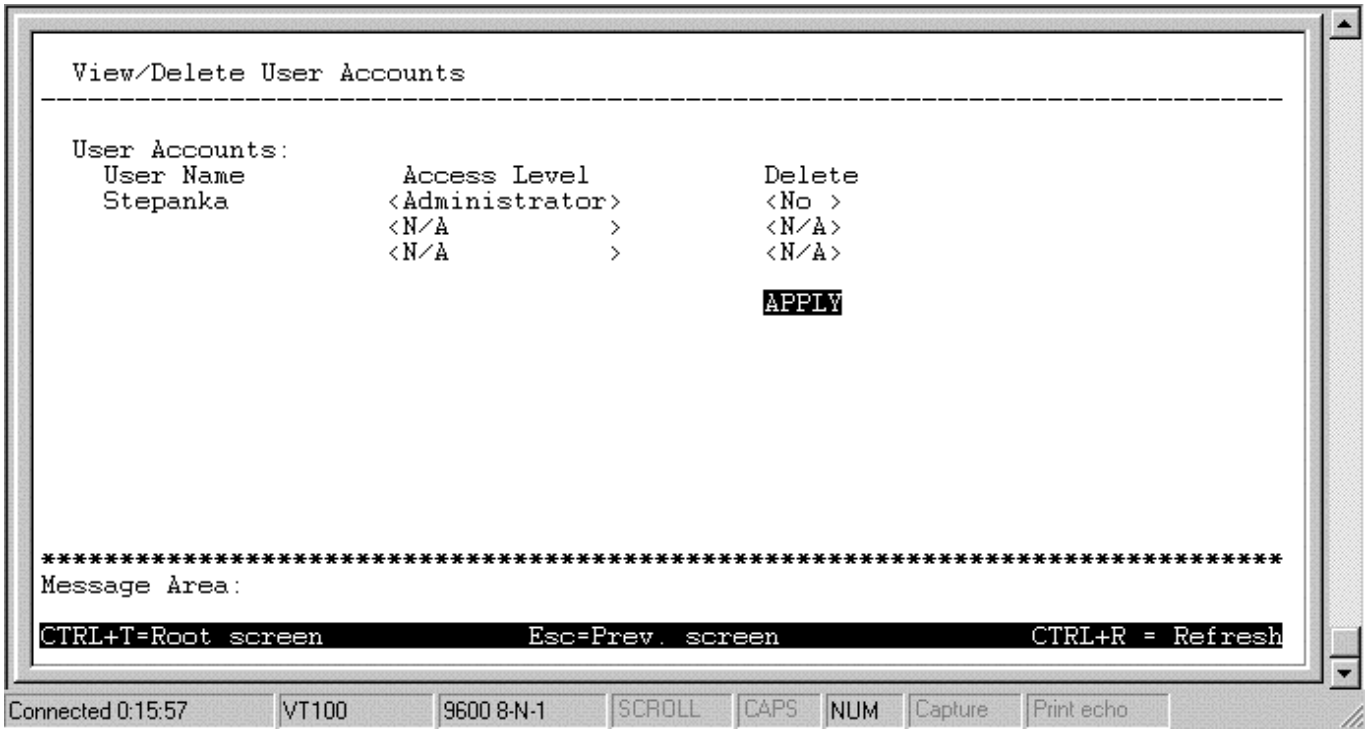


Figure 6-7. View/Delete User Accounts screen

To delete your user password:

1. Toggle the Delete field of the user you wish to remove to *Yes*.
2. Press APPLY to let the user deletion take effect.

Setting Up The Switch

This section will help prepare the Switch user by describing the **Configuration**, **Update Firmware and Configuration Files**, **Save Changes**, and **System Utilities** menus and their respective sub-menus.

Configuration

Choose **Configuration** to access the first item on the DES-3225G main menu. The following menu appears:

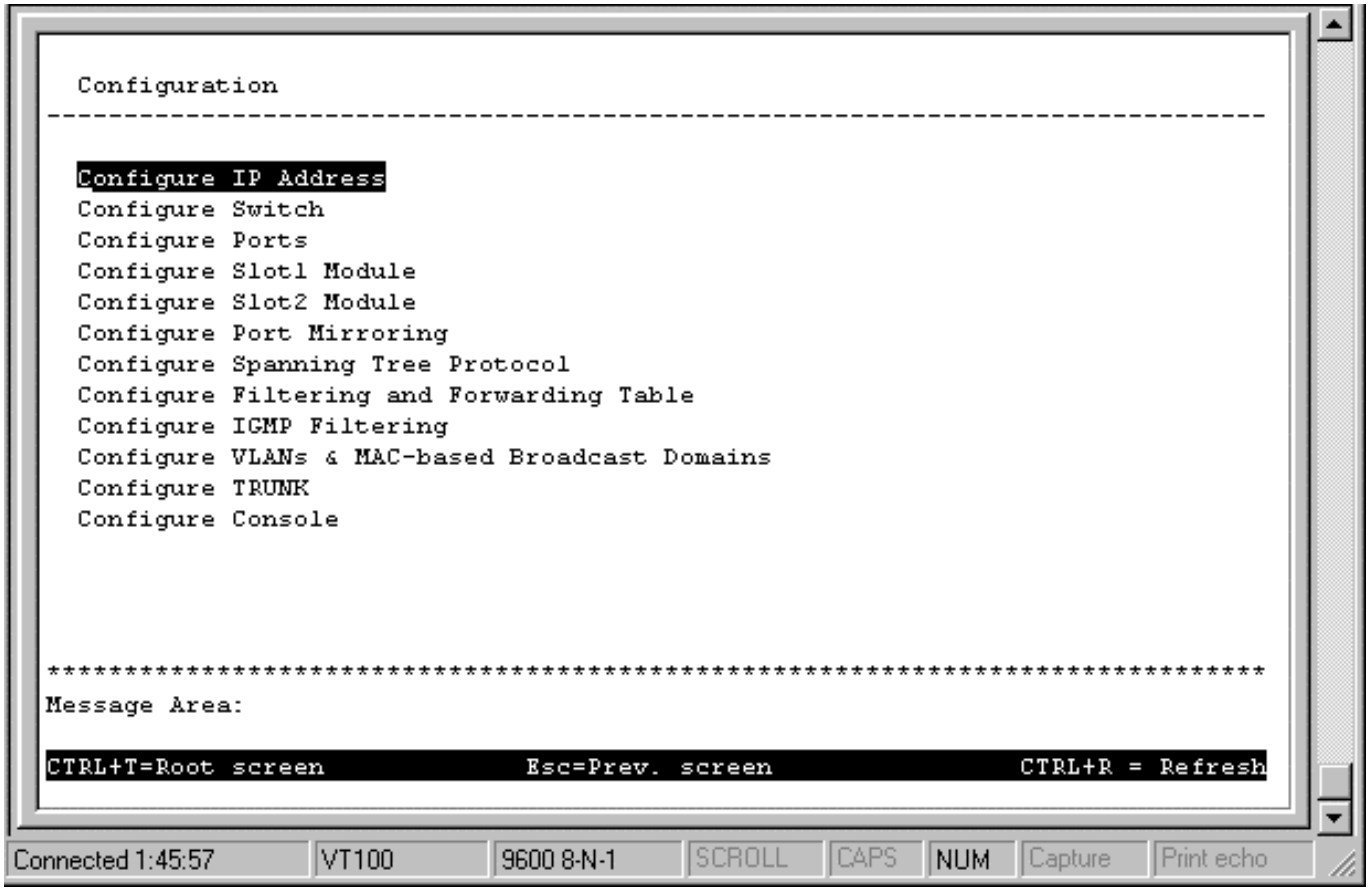


Figure 6-8. Configuration menu

You will need to change some settings to allow you to be able to manage the Switch from an SNMP-based Network Management System such as SNMP v1 or to be able to access the Switch using the Telnet protocol. See the next chapter for Web-based network management information.

Configure IP Address

The Switch needs to have an IP address assigned to it so that an In-Band network management system or Telnet client can find it on the network. The **IP Configuration** screen allows you to change the settings for the two different interfaces used on the Switch: the Ethernet interface used for in-band communication, and the SLIP interface used over the console port for out-of-band communication.

Choose **Configure IP Address** to access the first item on the **Configuration** menu. The following screen appears:

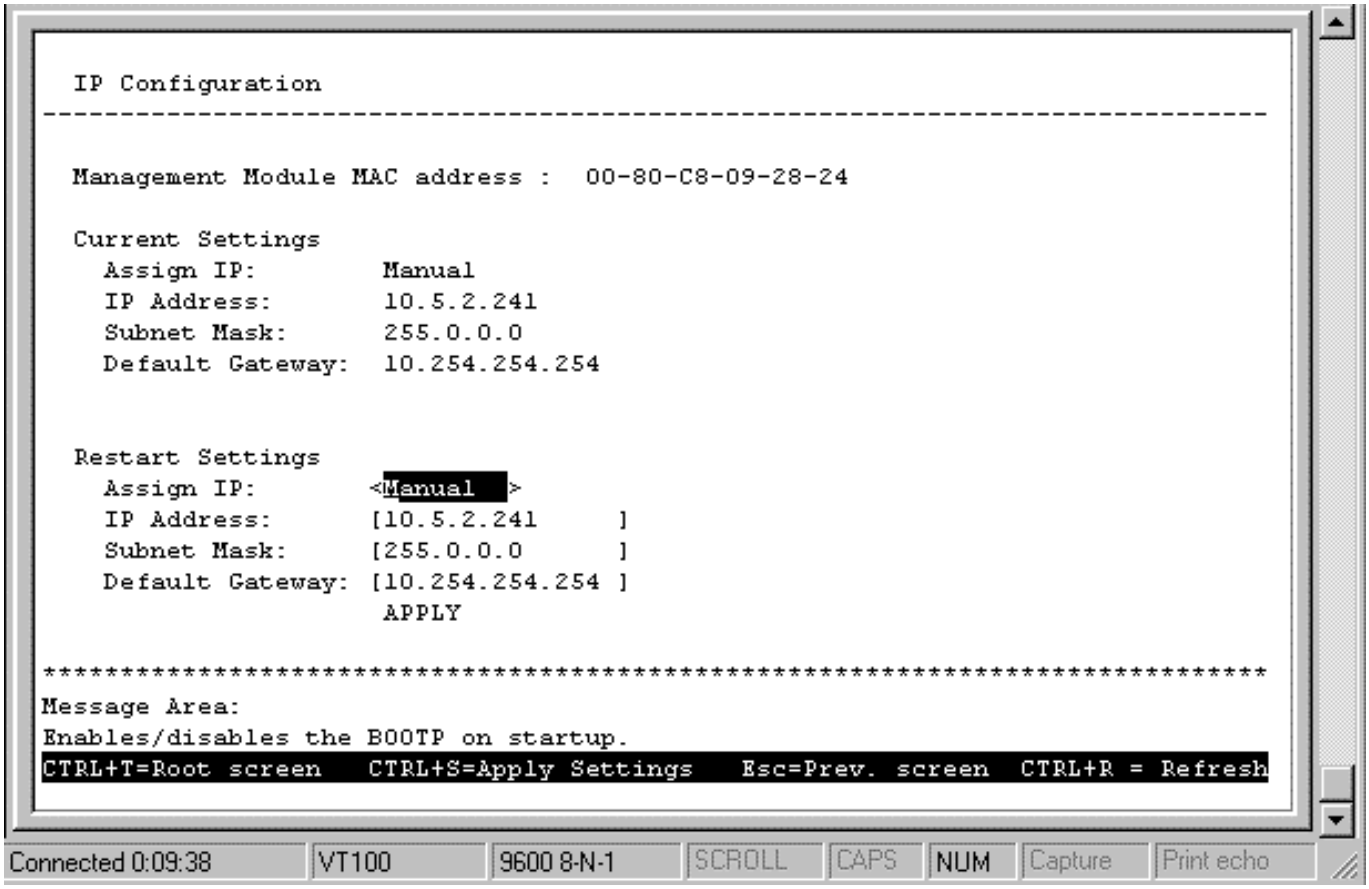


Figure 6-9. IP Configuration screen

The fields listed under the Current Settings heading are those that are currently being used by the Switch. Those fields listed under Restart Settings will be used after the Switch has been Reset. Fields that can be set include:

- **Assign IP** Determines whether the Switch should get its IP Address settings from the user (*Manual*), a *BOOTP* server, or a *DHCP* server. If *Manual* is chosen, the Switch will use the IP Address, Subnet Mask and Default Gateway settings defined in this screen upon being rebooted. If *BOOTP* is chosen, the Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the supplied settings. If *DHCP* is chosen, a Dynamic Host Configuration Protocol request will be sent when the Switch is powered up.

- **IP Address** Determines the IP address used by the Switch for receiving SNMP and Telnet communications. These fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. This address should be a unique address on a network assigned to you by the central Internet authorities. The same IP address is shared by both the SLIP and Ethernet network interfaces.

- **Subnet Mask** Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. If no subnetting is being done, the value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network.

- **Default Gateway** IP address that determines where frames with a destination outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your

network is not part of an internetwork, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

Configure Console

You can use the **Console Options** screen to choose whether to use the Switch's RS-232C serial port for console management or for out-of-band TCP/IP communications using SLIP, and to set the bit rate used for SLIP communications.

Choose **Configure Console** to access the last item on the **Configuration** menu. The following screen appears:

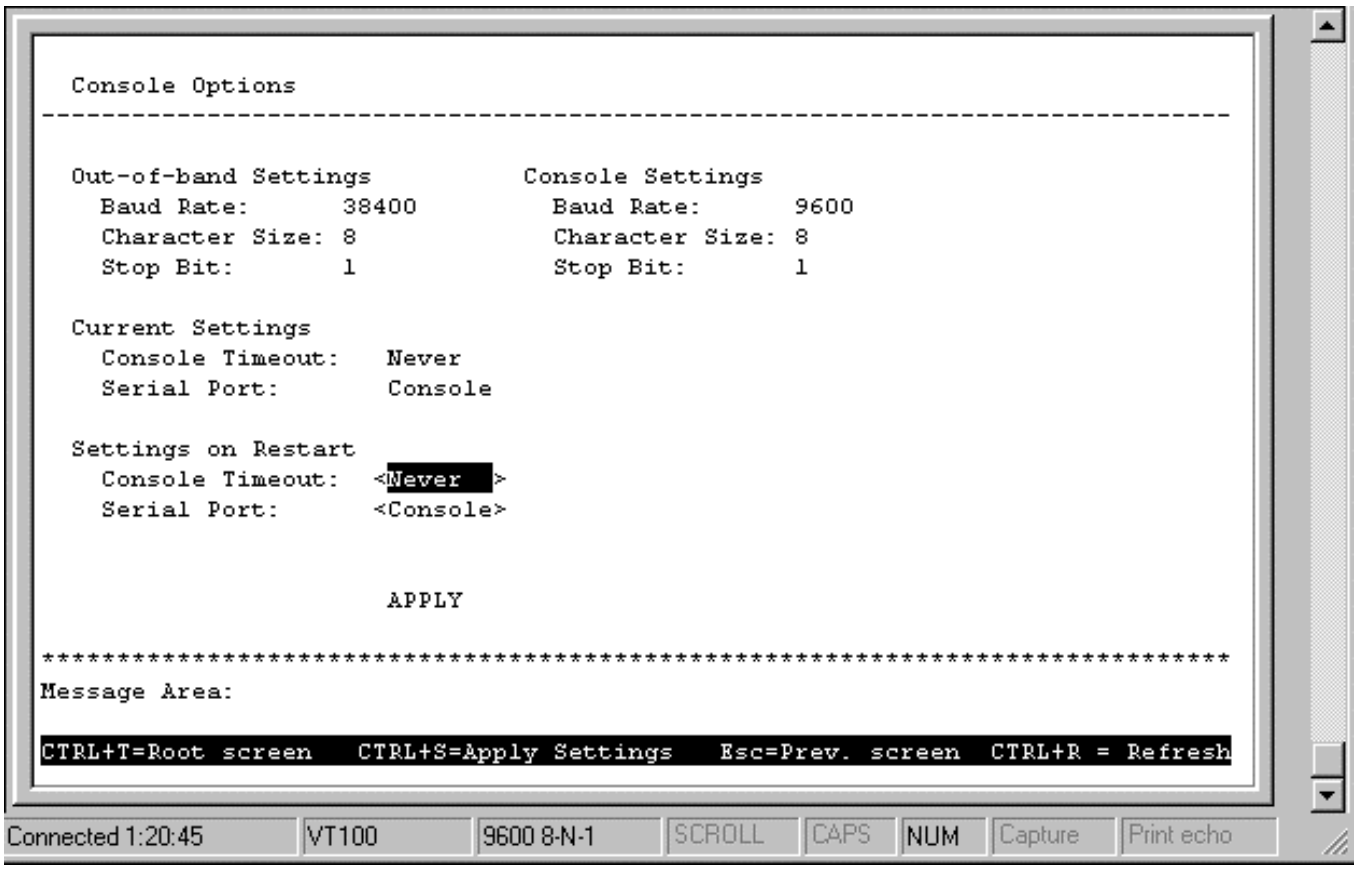


Figure 6-10. Console Options screen

The following fields can be set:

Settings on Restart:

- **Console Timeout** This setting for the restart of the console is *2 mins*, *5 mins*, *10 mins*, *15 mins*, or *Never*.
- **Serial Port** Determines whether the serial port should be used for out-of-band (SLIP) management or for console management, starting from the next time the Switch is restarted. In this field, you can toggle between *SLIP* or *Console* port type settings.
- **Baud Rate** Determines the serial port bit rate that will be used the next time the Switch is restarted. Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are 2400, 9600, 19,200 and 38,400 bits per second. The default setting in this Switch version is 9600.

The top of the screen displays the current settings for **Console Timeout** and **Serial Port** as well as the **Baud Rate**, **Character Size**, and **Stop Bit** for Out of Band and Console settings, respectively.

Configure Switch

The **Switch Configuration** screen shows various pieces of information about your Switch, and allows you to set the **System Name**, **System Location**, and **System Contact**. These settings can be retrieved from the Switch using SNMP requests, allowing these settings to be used for network management purposes.

Choose **Configure Switch** to access the second item on the **Configuration** menu. The following screen appears:

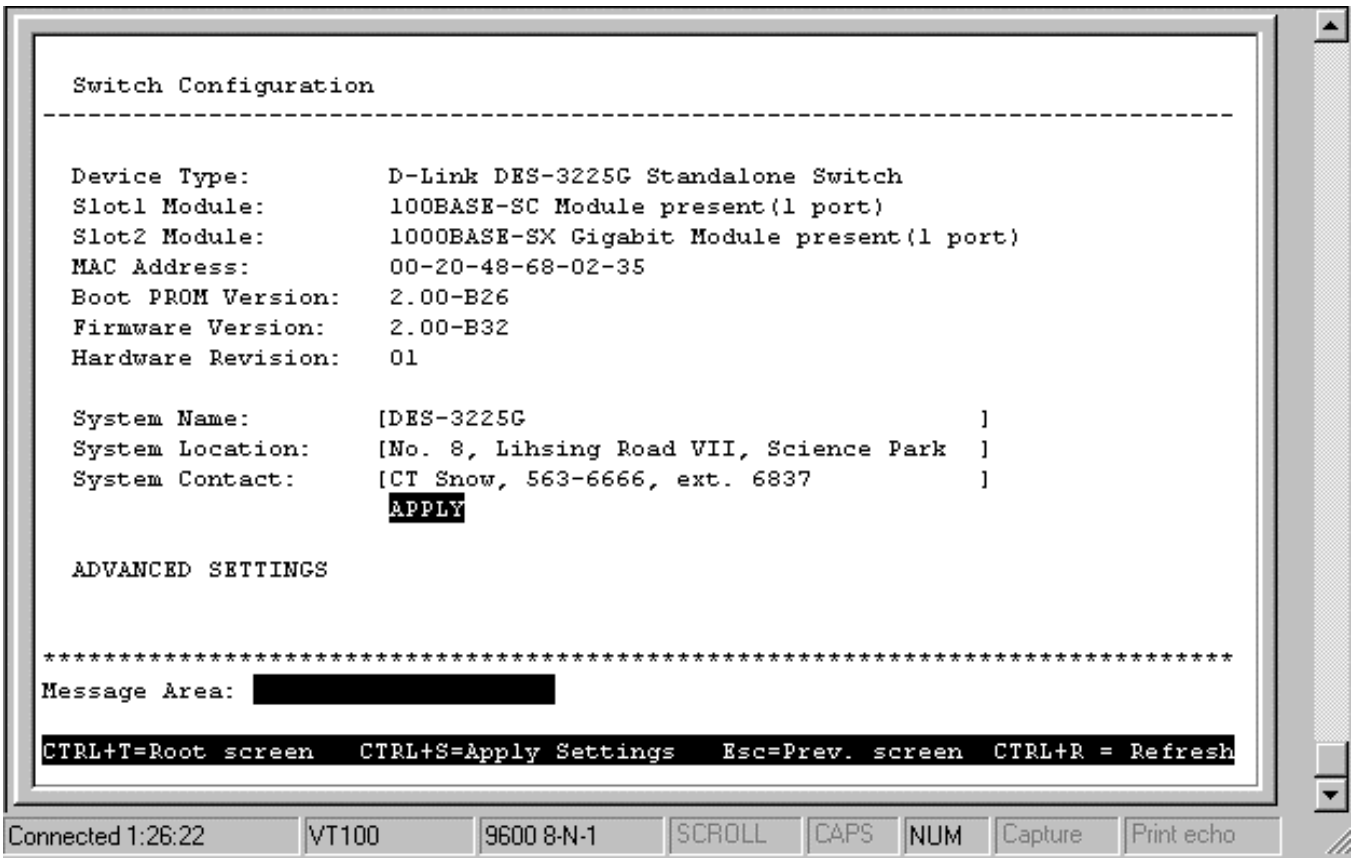


Figure 6-11. Switch Configuration screen

The fields you can set are:

- **System Name** Corresponds to the SNMP MIB II variable **`system.sysName`**, and is used to give a name to the Switch for administrative purposes. The Switch's fully qualified domain name is often used, provided a name has been assigned.
- **System Location** Corresponds to the SNMP MIB II variable **`system.sysLocation`**, and is used to indicate the physical location of the Switch for administrative purposes.
- **System Contact** Corresponds to the SNMP MIB II variable **`sysContact`**, and is used to give the name and contact information for the person responsible for administering the Switch.

Advanced Settings

The **Configure Advanced Switch Features** screen allows you to set an expiration time for MAC address entries and enable or disable auto-partitioning on all ports. Select ADVANCED SETTINGS on the **Switch Configuration** screen to access the **Configure Advanced Switch Features** screen (see below). Press APPLY once the desired changes have been made.

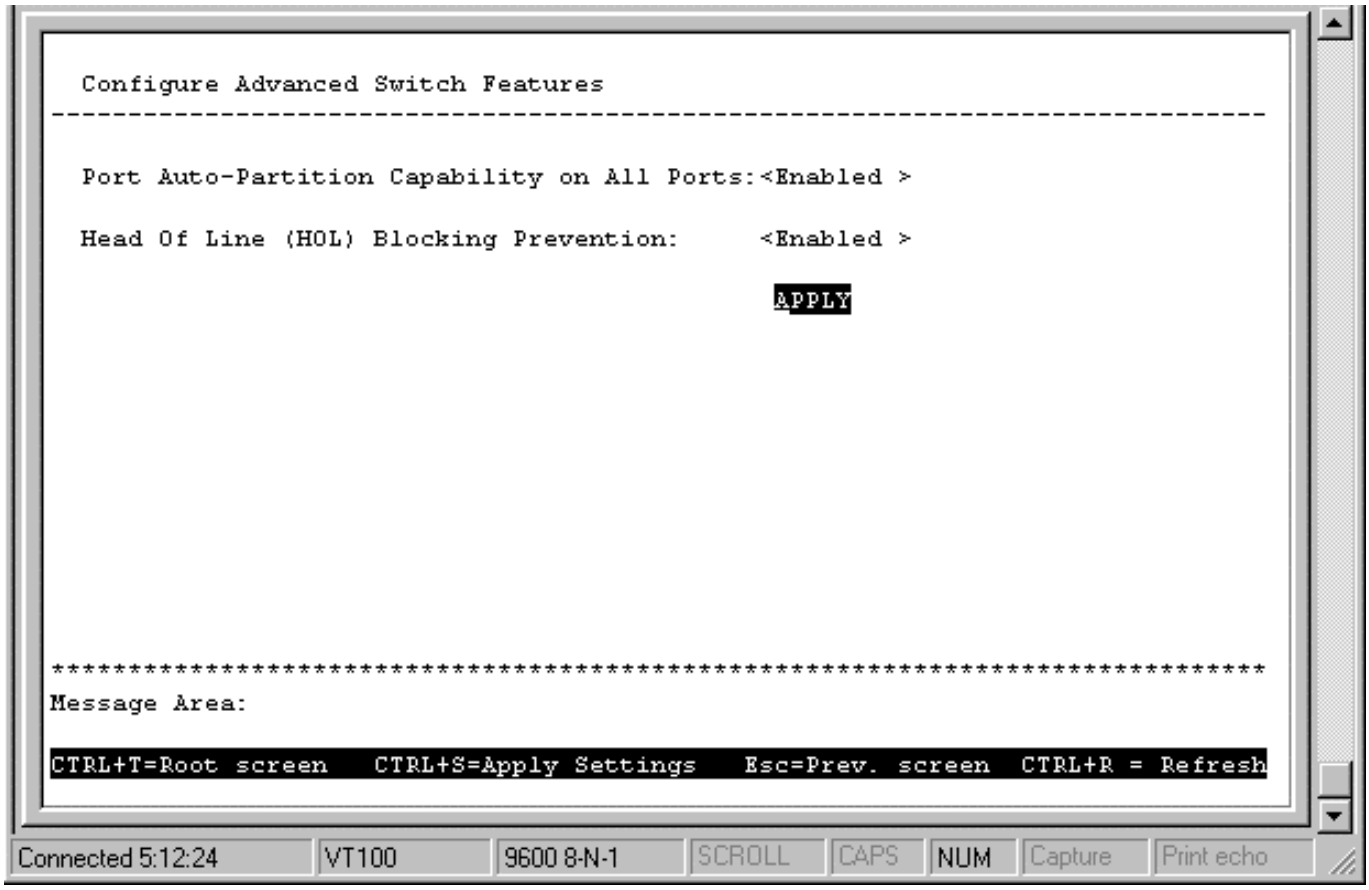


Figure 6-12. Configure Advanced Switch Features screen

The fields you can set are:

- **Port Auto-Partition Capability on All Ports** When this function is enabled, if too many consecutive collisions occur on an individual port, the port will be blocked off until a good packet is seen on the wire. If a port is partitioned, the Switch can only transmit data, not receive it.
- **Head Of Line (HOL) Blocking Prevention** Enables or disables Head-Of-Line Blocking Prevention. Head-of Line blocking occurs when a packet originating on Port 1, for instance, needs to be forwarded to Ports 2 and 3. If Port 2 is occupied (causing the packet to be held in memory until the port is free), the packet destined for Port 3 will also be delayed, even though the port may be free. Cumulatively, these delays can have a noticeable effect on overall network performance. Enabling HOL Blocking Prevention prevents Head-of-Line blocking from occurring, meaning that the packet destined for Port 3 gets delivered immediately.

Configure Ports

The port configuration screen allows you to change the port state in the case when you would like to partition a port due to excessive collision, or for observation, device repair, or security reasons. Great caution, however,

must be observed when partitioning a port; you should make sure that the partitioned port is not being used as the port to control or monitor the condition of other devices.

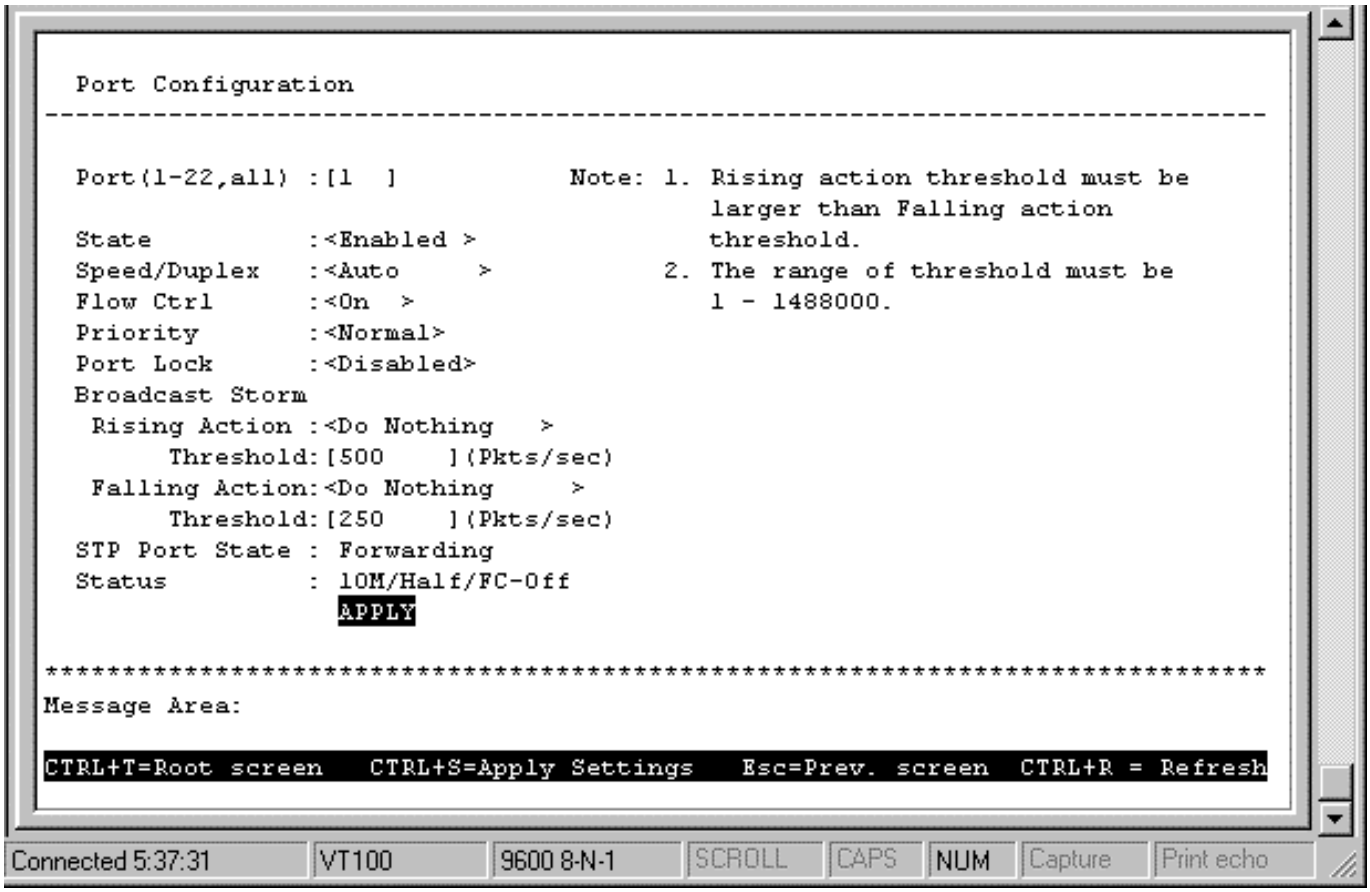


Figure 6-13. Port Configuration screen

Items in the above window are defined as follows:

- **Port** Specifies the port (1-22,all) that will be configured. When *all* is chosen, the settings you configure will be applied to all UTP ports.
- **State** Enables or disable*s* the port. This amounts to turning the port on or off.
- **Speed/Duplex** Selects the desired Speed and Duplex fort the port. Possible settings include: *Auto*, *100M/Full*, *100M/Half*, *10M/Full*, or *10M/Half*. Choosing *Auto* enables NWay auto-configuration on the port.
- **Flow Control** Toggles flow control *On* or *Off*. Flow control can only be used with other IEEE 802.3x-compliant devices and in a full-duplex connection. It is useful during periods of heavy network activity when the Switch's buffers can receive too much traffic and fill up faster than the Switch can forward the information. In such cases, the Switch will intervene and tell the transmitting device to pause to allow the information in the port buffer to be sent. When *Auto*-Negotiation is enabled in the Speed/Duplex field above, flow control will only be enabled if the connected device can Auto-negotiate flow control. Confirm that Flow Control is in force by checking the Status field.
- **Priority** Selects *Normal*, *High* or *Low*. The Switch has two packet queues where incoming packets wait to be processed for forwarding; a high priority and low priority queue. The high priority queue should only be used for data in which latency can have adverse affects on the function of an application, such as video or audio data, where latency can produce distorted sounds and images. Packets in the low priority queue will not be processed unless the High priority queue is empty. Setting the port priority to

high will deliver all packets arriving at the port to the high priority queue, a *low* setting will send them all to the low priority queue. The *Normal* settings causes the port to examine the packet for an IEEE 802.1p/Q priority tag. If no tag exists, the packet will be sent to the low priority queue. If the priority tag field in the packet header contains a value of 0-3, the packet will be placed in the low priority queue; a value of 4-7 causes the packet to be placed in the high priority queue.

- **Port Lock** When locked, automatic learning for all stations connected to this port will stop and entries in the Forwarding Table for all devices residing on this port will age out. The only traffic this port will allow is traffic from machines whose MAC address is manually entered in the Static Forwarding Table.

- **Broadcast Storm Rising Action** This setting will be activated when *Broadcast Storm Rising Threshold* (below) is met. When triggered, the port can be configured to *Do Nothing*, *Blocking* or *Blocking-Trap*. The *Do Nothing* setting causes the switch to operate normally, in other words, ignore the broadcast storm condition. The *Blocking* setting causes the port to drop all broadcast frames, thus isolating the broadcast storm. *Blocking-Trap* performs the same action as *Blocking*, except it also sends a trap to the designated Trap Recipient informing them of the situation. For more information on broadcast storms, please refer to the *Switch Management Concepts* section of this manual.

- **Broadcast Storm Rising Threshold** This setting defines a ceiling for the number of broadcast packets per second on this port. Once met, the *Broadcast Storm Rising Action* (above) will be triggered. The assigned number should be high enough to allow normal broadcast packets (which comprise significant traffic) to be let through, while being low enough so that broadcast storms can be detected early.

- **Broadcast Storm Falling Action** This setting will be activated when the *Broadcast Storm Rising Threshold* and then the *Broadcast Storm Falling Threshold* (below) is met. This setting can be configured to *Do Nothing*, *Forwarding* or *Forwarding-Trap*. The *Do Nothing* setting causes the switch to operate normally, in other words, ignore the situation. If the port had met the *Broadcast Storm Rising Action* criteria and started *Blocking* broadcast packets, it will continue doing so. The *Forwarding* setting causes the port to begin forwarding broadcast frames, thus removing the *Blocking* state imposed by the *Broadcast Storm Rising Action*. *Forwarding-Trap* performs the same action as *Forwarding*, except it also sends a trap to the designated Trap Recipient informing them of the situation.

- **Broadcast Storm Falling Threshold** This setting defines the number of broadcast packets per second on this port which will trigger the *Broadcast Storm Falling Action* (above). This threshold will only trigger an action if the *Broadcast Storm Rising Threshold* has first been reached. The assigned number should be high enough to allow normal broadcast packets (which comprise significant traffic) to be let through as early as possible, while being low enough so that broadcast storms are completely eliminated.

Press APPLY to let the changes take effect. If you wish these changes to be the default for the switch, return to the main menu and choose **Save Changes**.

STP Port State (whether the Spanning Tree Protocol is enabled or disabled on this port) and **Status** reflect the current conditions of the port. They are read-only fields and cannot be changed.

Configure Slot1 Module

This screen allows you to change the port state of the module in slot 1 in the case when you would like to partition a port due to excessive collision, or for observation, device repair, or security reasons. Great caution, however, must be observed when disabling a port, since all data passing through the port will be discarded by the Switch.

To change the configuration of the Slot1 module shown below:

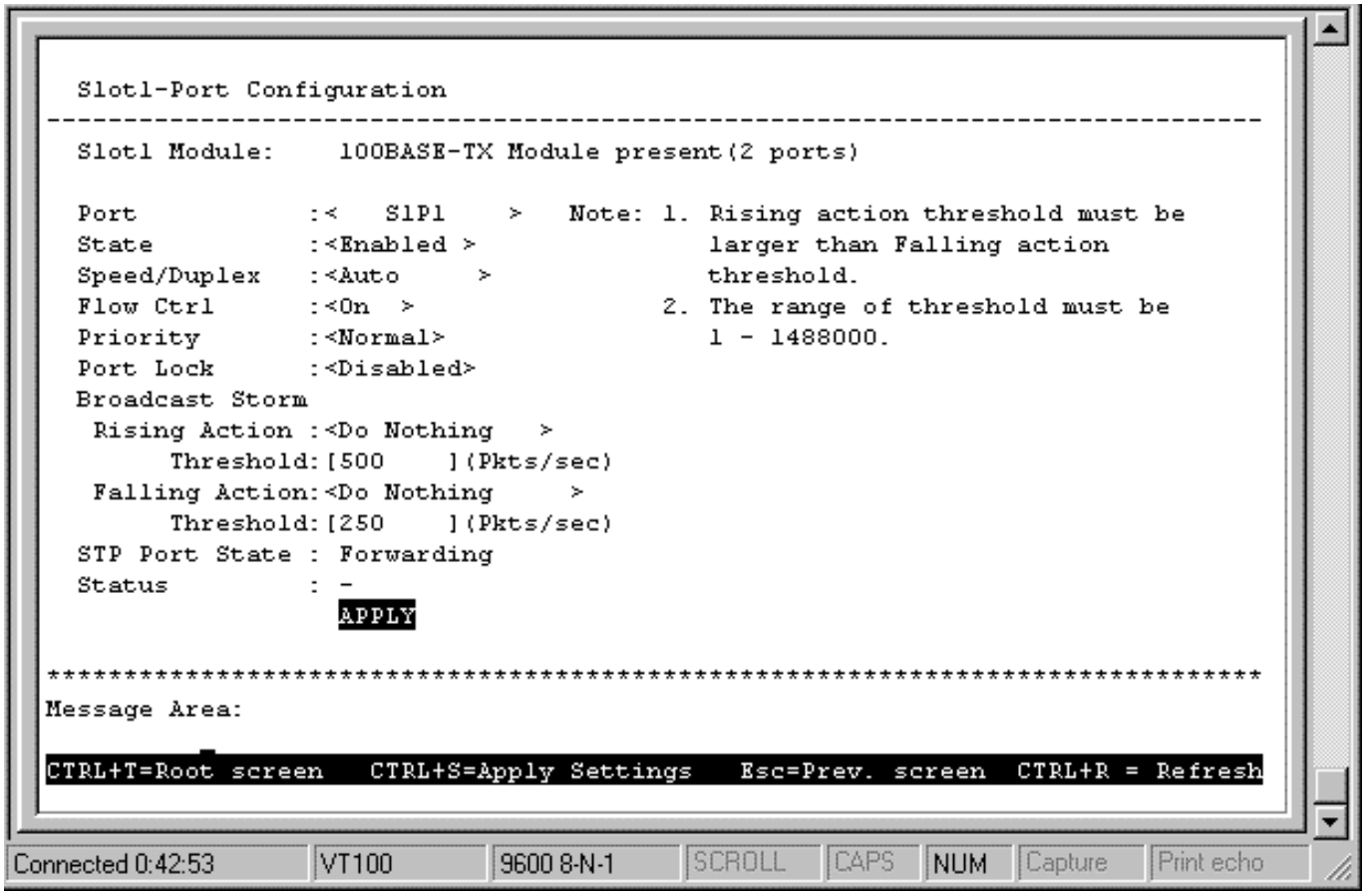


Figure 6-14. Slot1-Port Configuration screen

- **Port** Field specifies either *S1P1*, the Port 1x port or *S1P2*, the Port 2x port on the module. For single-port modules, only *S1P1* will be available.
- **State** Enables or disables this port.
- **Speed/Duplex** Selects the desired Speed and Duplex fort the port. Possible settings include: *Auto*, *100M/Full*, *100M/Half*, *10M/Full*, or *10M/Half*. Choosing *Auto* enables NWay auto-configuration on the port.
- **Flow Control** *Enables* or *disables* IEEE 802.1x full-duplex (only) flow control on this port. See *Flow Control* in the *Configure Ports* section above for a more detailed explanation.
- **Priority** Selects *Normal*, *High* or *Low*. See *Priority* in the *Configure Ports* section above for a more detailed explanation.
- **Port Lock** When *locked*, automatic learning for all stations connected to this port will stop and entries in the Forwarding Table for all devices residing on this port will age out. The only traffic this port will allow is traffic from machines whose MAC address is manually entered in the Static Forwarding Table.
- **Broadcast Storm Rising Action** Selects an action – *Do Nothing, Blocking, Blocking-Trap* – for the port when the Broadcast Storm Rising Threshold (below) condition is met. See *Broadcast Storm Rising Action* in the *Configure Ports* section of this manual for a more detailed explanation.
- **Broadcast Storm Rising Threshold** This setting defines a ceiling for the number of broadcast packets per second on this port. See *Broadcast Storm Rising Threshold* in the *Configure Ports* section of this manual for a more detailed explanation.

- **Broadcast Storm Falling Action** This setting will be activated when the *Broadcast Storm Rising Threshold* and then the *Broadcast Storm Falling Threshold* (below) is met. This setting can be configured to *Do Nothing*, *Forwarding* or *Forwarding-Trap*. See *Broadcast Storm Falling Action* in the *Configure Ports* section of this manual for a more detailed explanation.

- **Broadcast Storm Falling Threshold** This setting defines the number of broadcast packets per second on this port which will trigger the *Broadcast Storm Falling Action* (above). See *Broadcast Storm Falling Threshold* in the *Configure Ports* section of this manual for a more detailed explanation.

Press APPLY to have the changes take effect.

STP Port State and **Status** reflect the current conditions of the port. They are read-only fields and cannot be changed.

Configure Slot2 Module

This screen allows you to change the port state of an optional Gigabit Ethernet module in slot 2. This is useful in the case when you would like to partition a port due to excessive collision, or for observation, device repair, or security reasons. Great caution, however, must be observed when disabling a port, since all data passing through the port will be discarded by the Switch.

The **Configure Slot2 Module** screen appears as follows:

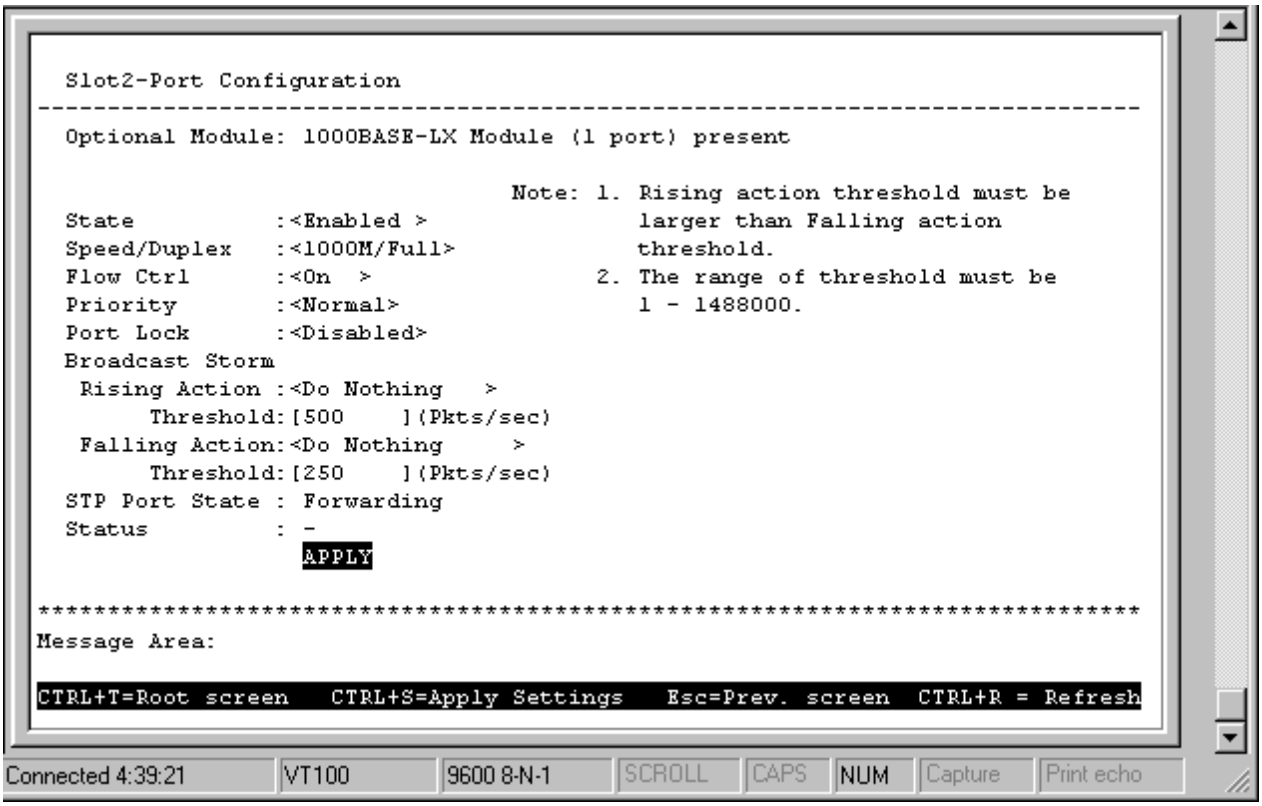


Figure 6-15. Slot2-Port Configuration screen

- **State** Enables or disables this port.

- **Speed/Duplex** If either a 1000BASE-SX or 1000BASE-LX module is used, this field will offer two choices: *1000M/Full* or *Auto*. If a 1000BASE-T module is used, this field will offer the following choices: *1000M/Full*, *100M/Full*, *100M/Half*, and *Auto*. Please note that DES-3251G/GL version A2 supports *1000M/Full* only. Version A3 supports *1000M/Full* and *Auto*.

- **Flow Control** Enables or disables IEEE 802.1x full-duplex (only) flow control on this port. See *Flow Control* in the *Configure Ports* section above for a more detailed explanation.
- **Priority** Selects *Normal*, *High* or *Low*. See *Priority* in the *Configure Ports* section above for a more detailed explanation.
- **Port Lock** When *locked*, automatic learning for all stations connected to this port will stop and entries in the Forwarding Table for all devices residing on this port will age out. The only traffic this port will allow is traffic from machines whose MAC address is manually entered in the Static Forwarding Table.
- **Broadcast Storm Rising Action** Selects an action – *Do Nothing, Blocking, Blocking-Trap* – for the port when the Broadcast Storm Rising Threshold (below) condition is met. See *Broadcast Storm Rising Action* in the *Configure Ports* section of this manual for a more detailed explanation.
- **Broadcast Storm Rising Threshold** This setting defines a ceiling for the number of broadcast packets per second on this port. See *Broadcast Storm Rising Threshold* in the *Configure Ports* section of this manual for a more detailed explanation.
- **Broadcast Storm Falling Action** This setting will be activated when the *Broadcast Storm Rising Threshold* and then the *Broadcast Storm Falling Threshold* (below) is met. This setting can be configured to *Do Nothing*, *Forwarding* or *Forwarding-Trap*. See *Broadcast Storm Falling Action* in the *Configure Ports* section of this manual for a more detailed explanation.
- **Broadcast Storm Falling Threshold** This setting defines the number of broadcast packets per second on this port which will trigger the *Broadcast Storm Falling Action* (above). See *Broadcast Storm Falling Threshold* in the *Configure Ports* section of this manual for a more detailed explanation.

Press APPLY to have the changes take effect.

STP Port State and **Status** reflect the current conditions of the port. They are read-only fields and cannot be changed.

Configure Port Mirroring

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

Choose **Configure Port Mirroring** on the **Configuration** menu to access the following screen:

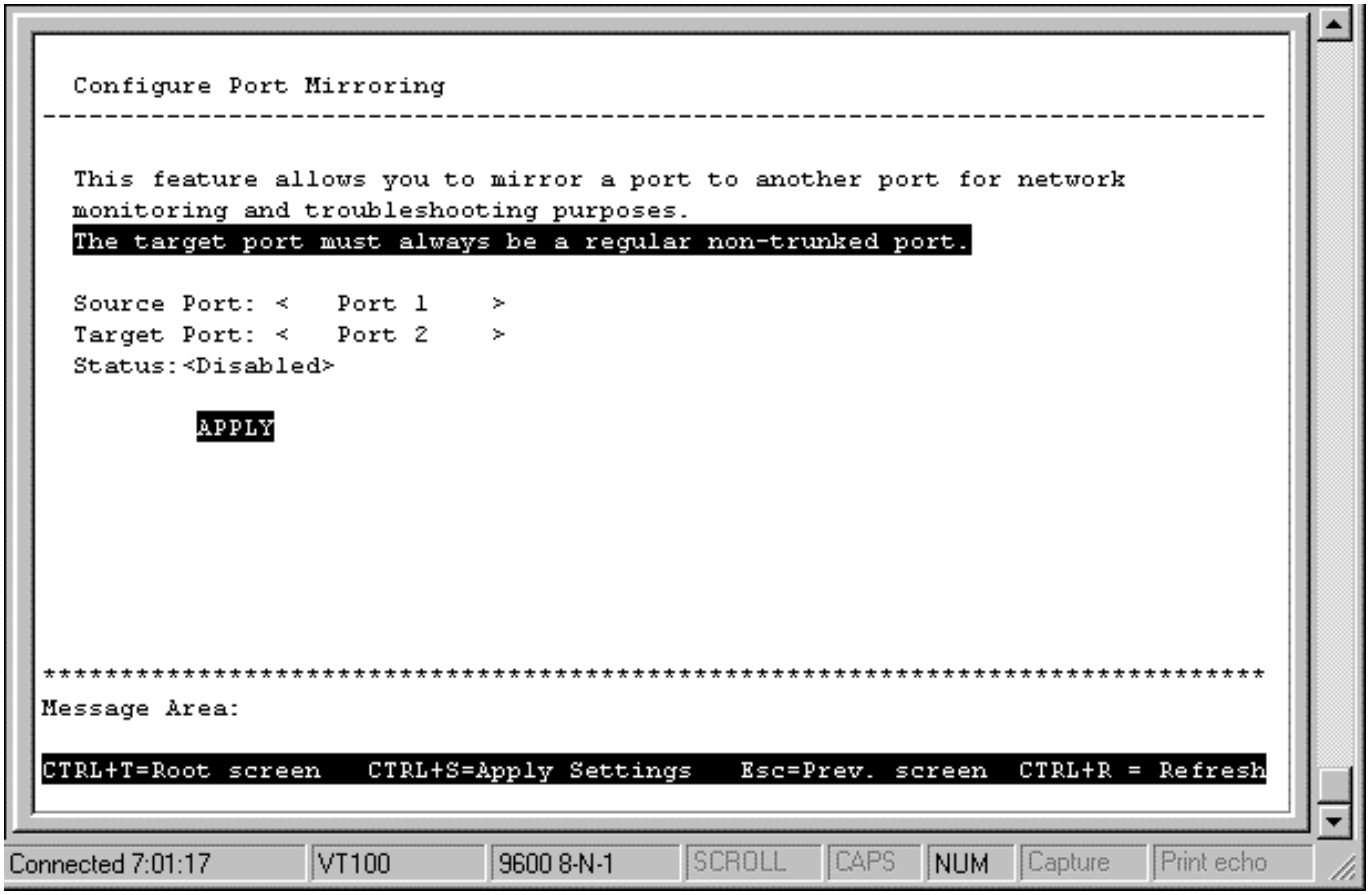


Figure 6-16. Configure Port Mirroring screen

To configure a mirror port, select the port from where you want to copy frames in the Source Port field. Then select the port which receives the copies from the source port in the Target Port field. The target port is where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe.

Note: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port cannot be a member of a trunk group.

Configure Spanning Tree Protocol

The Spanning Tree Algorithm Parameters can be used for creating alternative paths in your network. The Protocol Parameters allow you to change the behind the scene parameters of the Spanning Tree Algorithm at the bridge level. The parameters for this section have been fully explained in Chapter 5's *Switch Management Concepts*, see *STA Operation Levels: On the Bridge level*, and *User-Changeable Parameters*. It is recommended that you read these sections, as well as the introductory section in the same chapter entitled *Spanning Tree Algorithm* before changing any of the parameters.

STP Parameter Settings

To change the Protocol Parameters:

1. Choose **Configure Spanning Tree Protocol** from the **Configuration** menu. The following **Configure Spanning Tree Protocol** menu will be displayed:

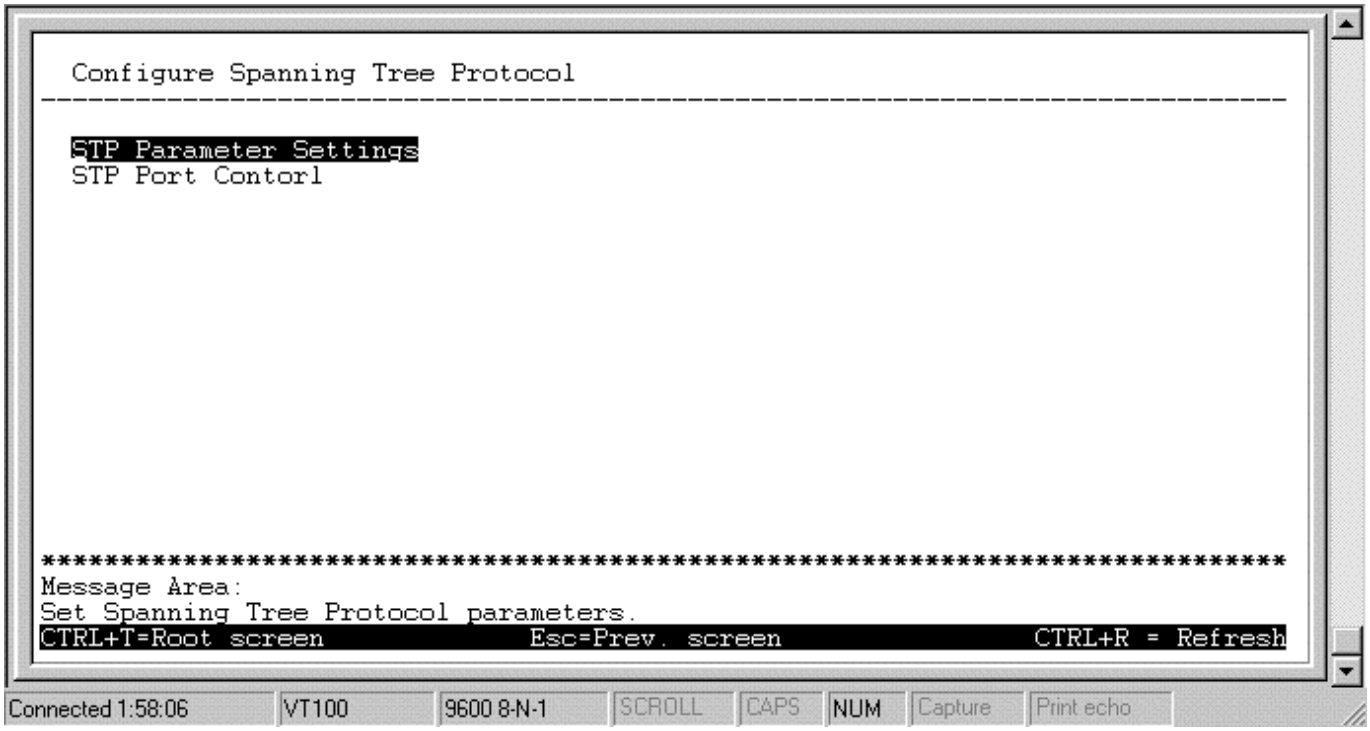


Figure 6-17. Configure Spanning Tree Protocol menu

2. Choose **STP Parameter Setting** to access the following screen:

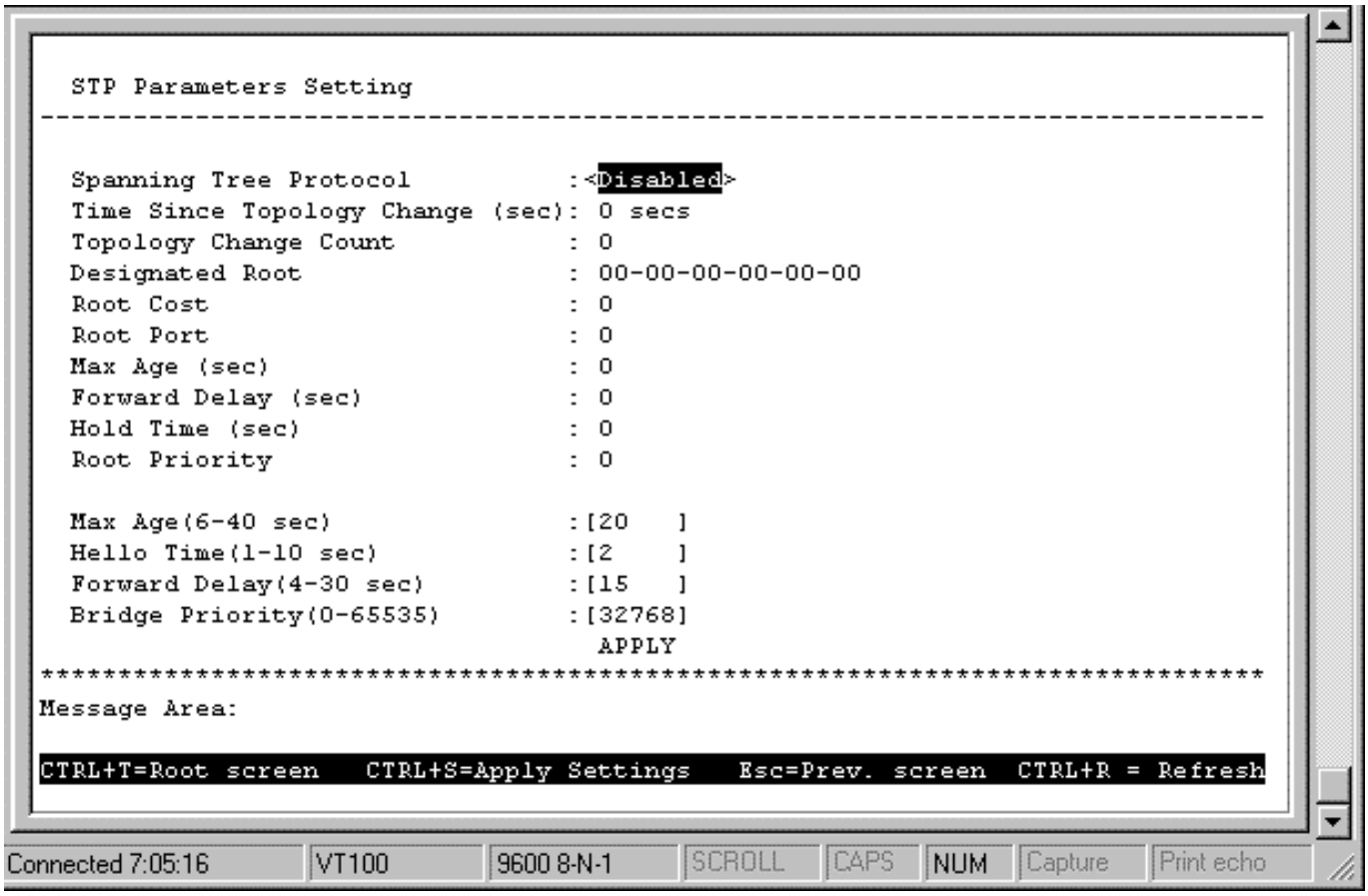


Figure 6-18. STP Parameters Setting screen

The information on the screen is described as follows:

- **Spanning Tree Protocol** Enables or disables the Spanning Tree Protocol.
- **Time Since Topology Changes (sec)** Read-only object displays the last time changes were made to the network topology. These changes usually occur when backup paths are activated due to primary path failures.
- **Topology Change Count** Read-only object displays the number of times (since the current management session with the device was started) changes were made to the network topology. Changes usually occur on the network when backup paths are activated.
- **Designated Root** Read-only object displays the MAC (Ethernet) address of the bridge/switch on the network that has been chosen as the STP root.
- **Root Cost** Read-only object displays the cost for the path between the switch and the root bridge. If the switch is the root bridge, then the root cost is zero.
- **Root port** Read-only object identifies the port (on the bridge) that offers the least path cost from the bridge to the root bridge. In the event of a network loop, data packets will pass through the root port.
- **Max Age (sec)** Read-only object indicates the maximum age of STP information learned from the network (on any port) before it is discarded.
- **Forward Delay (sec)** Read-only object indicates how fast any port on the bridge can change its spanning state when moving towards the forwarding state. The value determines how long the port stays in each of the listening and learning states, which precede the forwarding state.
- **Hold Time (sec)** Read-only object displays the time interval during which no more than two configuration BPDUs shall be transmitted by the bridge.
- **Root Priority** Read-only object displays the priority number of the root bridge of the Spanning Tree. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multi-bridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. A bridge priority ranges from 0 to 65535, with 0 being the highest priority.
- **Max Age (6-40 sec)** Maximum Age is a read-write object that can be set from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root ridge, your Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.
- **Hello Time (1-10 sec)** Hello Time is a read-write object that can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.
- **Forward Delay (4-30 sec)** The Forward Delay is a read-write object that can be set from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.
- **Bridge Priority (0-65535)** A Bridge Priority is a read-write object that can be set from 0 to 65535. This is the priority number of the bridge. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multibridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. Zero is the highest priority.

STP Port Control

To change the parameters on individual ports:

1. Choose **Configure Spanning Tree Protocol** from the **Configuration** menu.
2. Choose **STP Port Control** from the **Configure Spanning Tree Protocol** menu. The following screen appears:

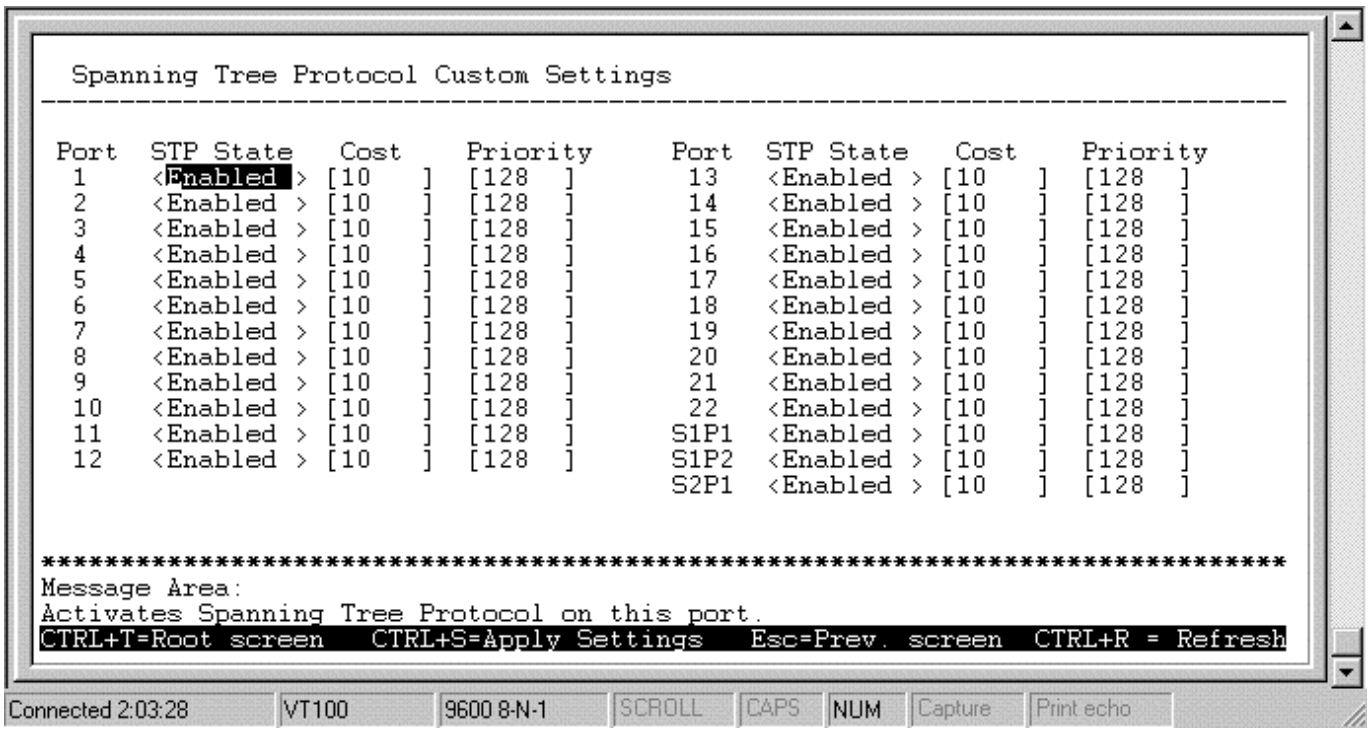


Figure 6-19. Spanning Tree Protocol Custom Settings screen

Items in the above window are described as follows:

- **STP State** Enables or disables the Spanning Tree Protocol on a particular port.
- **Cost** This is a read-only object. Both 10Mbps and 100Mbps segments have an assigned Path Cost of 19, based on the STA specifications.
- **Priority** Port Priority is a read-write object that can be set from 0 to 255. This is the priority number of the port. The lower the port priority, the more chance the bridge has of becoming the root port. Zero is the highest priority.

Configure Filtering and Forwarding Table

When a packet hits the Switch, it looks in the filtering and forwarding table to decide what to do with the packet; either to filter it off the network, or to forward it through the port on which its destination lies.

Dynamic Filtering and Static Filtering are among the two important features of the **Custom Filtering Table**. They are defined here briefly as follows. *Dynamic Filtering* is defined when a dynamic entry is created by the Learning Process as a result of observation of network traffic in the Filtering Database. *Static Filtering* is defined as static entries that may be added and removed from the Filtering Database by the user. They are not automatically removed by any timeout mechanism.

The **Configure Filtering and Forwarding Table** screen allows you to allows you to stop or start address learning, change the way the Switch treats MAC address table entries, and select an age-out time of the MAC address in the selected address table. This screen also permits you to access three additional configuration screens from the menu at the bottom of the screen.

Choose **Configure Filtering and Forwarding Table** from the **Configuration** menu to access the following screen:

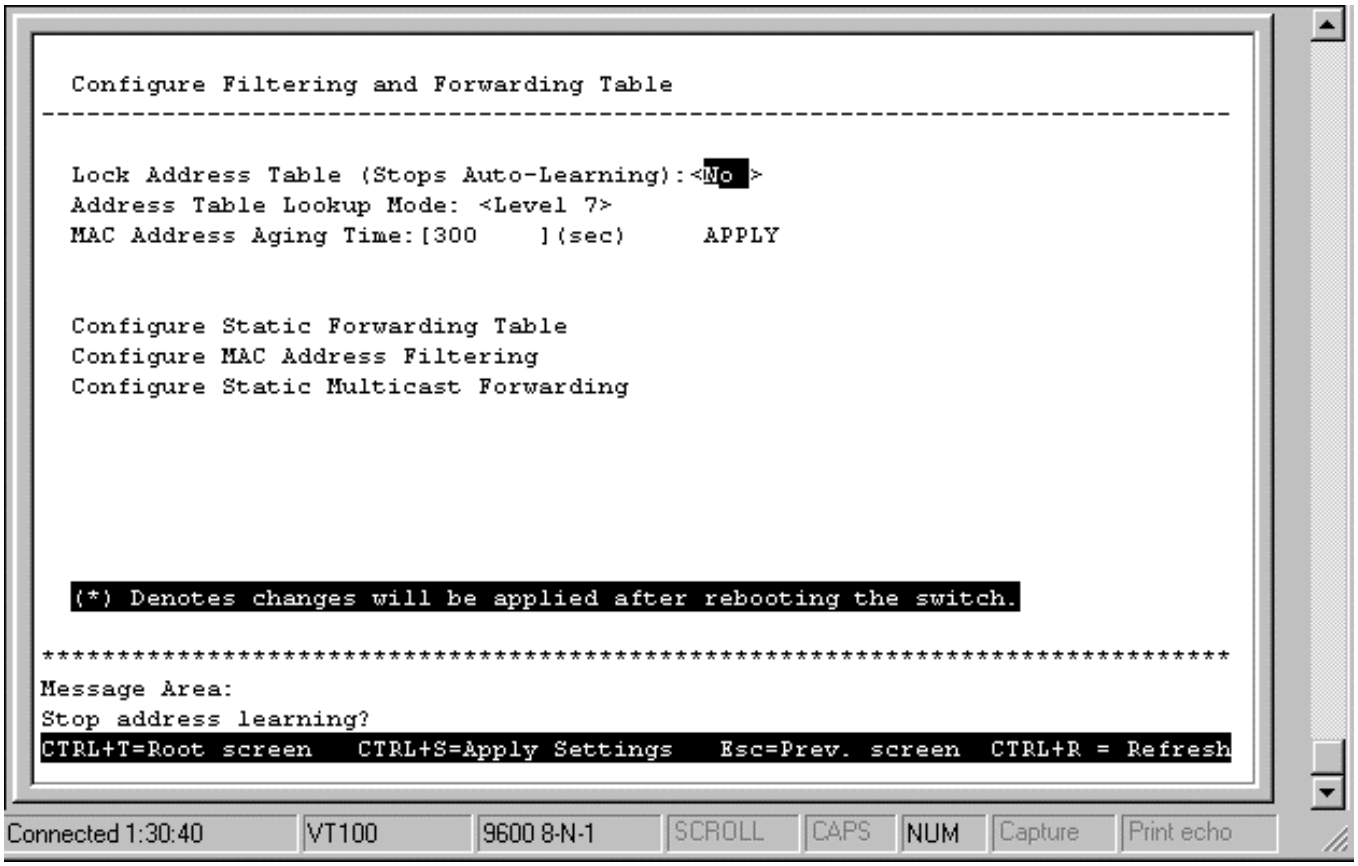


Figure 6-20. Configure Filtering and Forwarding Table screen

The following fields at the top of the screen can be set:

- **Lock Address Table (Stops Auto-Learning)** Mostly used for security purposes, when the forwarding table is locked the Switch will no longer learn the MAC addresses for new hosts. If your network configuration doesn't change, locking the forwarding table helps keep intruders off your network since any packet coming from an unknown source address will be dropped by the Switch.

- **Address Table Lookup Mode** This setting allows the user to tailor the MAC address look up procedure. Choices are *Level 0, Level 1*, *Level 2*, *Level 3*, *Level 4*, *Level 5*, *Level, 6, Level 7*. The higher the level, the more MAC addresses can be learned by the Switch. However, a side effect is that throughput will be degraded the higher the level you select. *Level 1* is the default.

- **MAC Address Aging** Enter the desired MAC address age-out time in this field (10 to 1000000 seconds).

Please refer to the Packet Forwarding section of the *"Switch Management Concepts"* chapter of this manual for more detailed information.

Configure Static Forwarding Table

The **Static Forwarding Table** displays a list of manually defined static MAC address entries.

To access the **Custom Forwarding Table**, choose **Configure Filtering and Forwarding Table** from the **Configuration** menu. Then select **Configure Permanent Address Table Entry** from the bottom of the **Configure Filtering and Forwarding table** screen. The following screen appears:

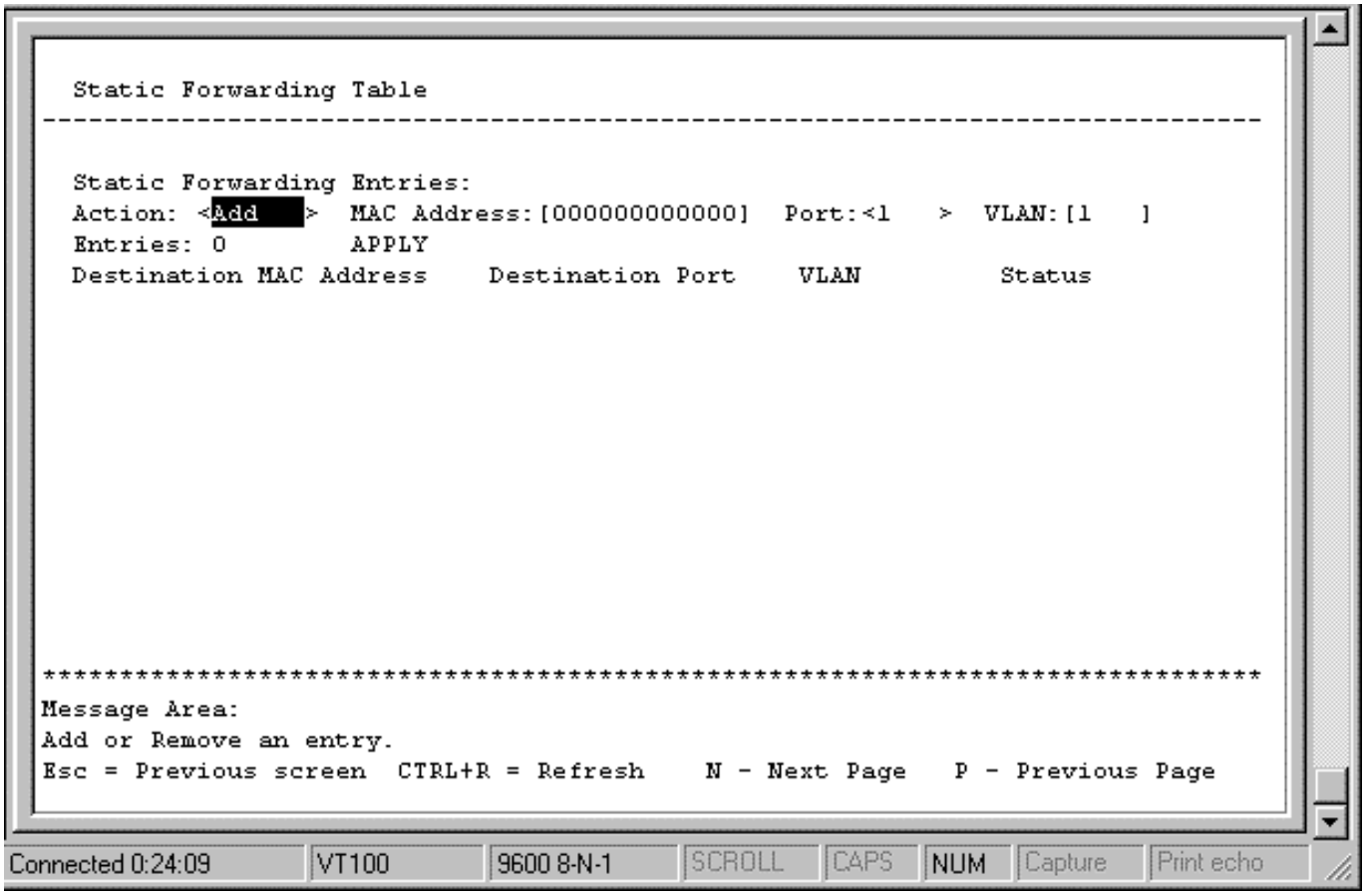


Figure 6-21. Static Forwarding Table screen

By mapping a MAC address to a destination port, the Switch can permanently forward traffic for a specified device through a specific port, even after long periods of network inactivity or during times of network congestion.

The following fields at the top of the screen can be set:

- **Action** Choose to *Add* or *Remove* an entry from the table.
- **MAC Address** A total of ten destination addresses per page will be seen. The Switch can hold up to 256 entries. This is the MAC address of the device that you are creating a permanent forwarding address for.
- **Port** Heading a port number will be displayed for each corresponding destination address. The Switch will always forward traffic to the specified device through this port.
- **VLAN** This setting only appears when Port-based or IEEE 802.1Q VLANs are active and defines the VLAN ID number in the packet. Make sure the port can accept packets on this VLAN by assigning the port this VID number.

Entries, as well as **Destination MAC Address**, **Destination Port**, **VLAN**, and **Status**, all in the lower part of the screen, are read-only. The **Status** of the static forwarding table entry can be *In use* or *Not apply*. *Not apply* means that there is a static filter for the same MAC address. Static filters always take

precedence over static forwarding entries. The switch will automatically upgrade the Status to "in use" once the static filter is removed.

Configure MAC Address Filtering

The **Static Filtering Table** contains filtering information configured into the Switch by (local or network) management specifying destination addresses which are not allowed to be forwarded. The Switch will check both the destination and source MAC addresses on all packets.

To access the **Static Filtering Table**, select **Configure Filtering and Forwarding Table** from the **Configuration** menu. Then select **Configure MAC Address Filtering** from the bottom of the **Configure Filtering and Forwarding Table** screen. The following screen appears:

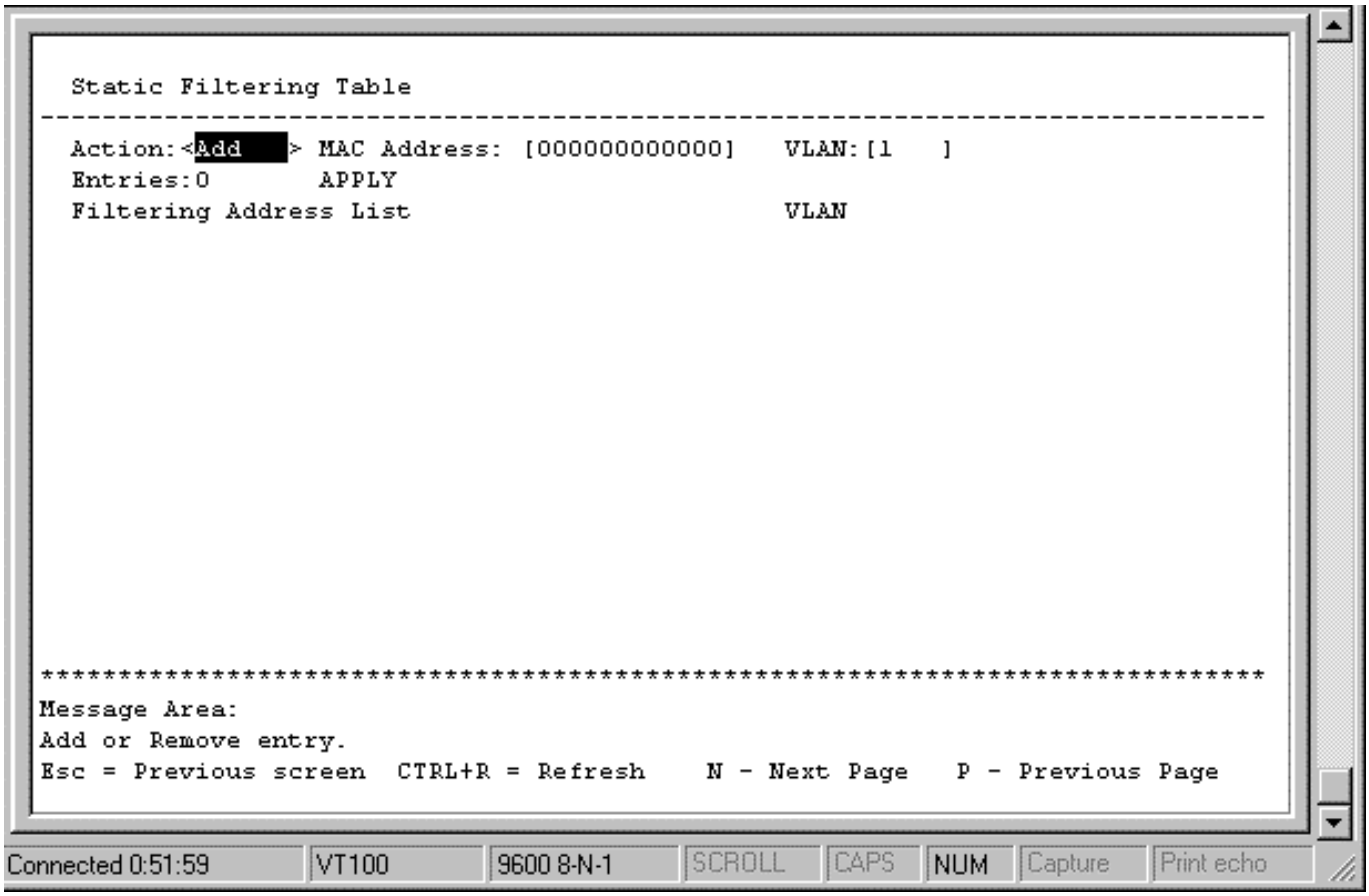


Figure 6-22. Static Filtering Table screen

To make a change to the **Static Filtering Table**, choose *Add* or *Remove* in the **Action** field. Then enter the **MAC Address** and **VLAN** (if Port-based or IEEE 802.1Q VLANs are enabled) and press APPLY.

Configure IGMP Filtering

Internet Group Management Protocol (IGMP) allows multicasting on your network. When IP Multicast Filtering is *Enabled*, the Switch can intelligently forward (rather than broadcasting) IGMP queries and reports sent between devices connected to the Switch and an IGMP-enabled device hosting IGMP on your network. When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa.

Basically, in these submenus you define whether the Switch can intelligently forward IGMP packets, and you must also define which 802.1Q VLANs (if present) can send and receive IGMP and Multicast packets.

To access the **IGMP Configuration** screen, choose **Configure IGMP Filtering** from the **Configuration** menu. The follow screen appears:

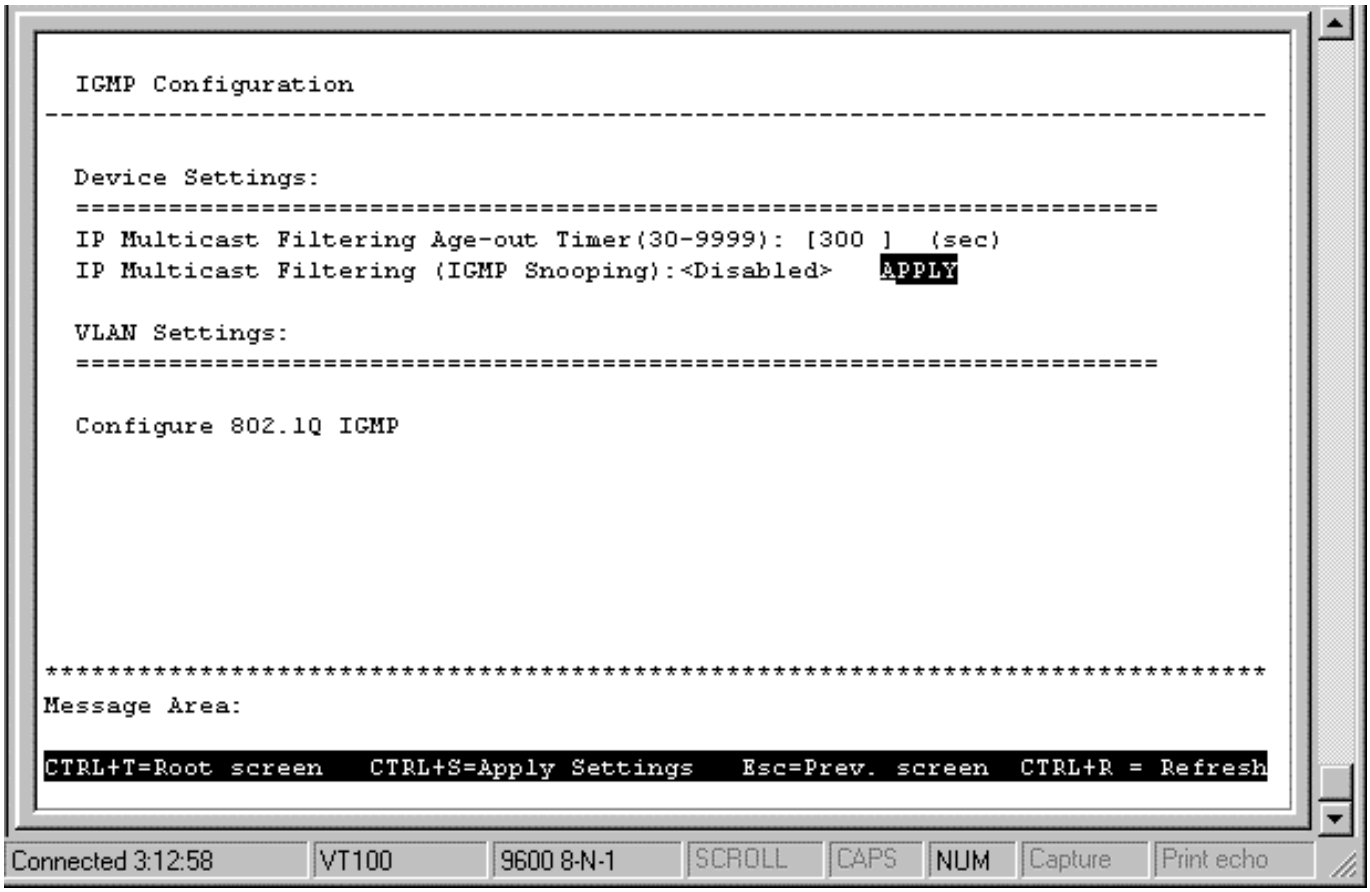


Figure 6-23. IGMP Configuration screen

Items in the above window are defined as follows:

- **IP Multicast Filtering Age-out Timer(30-9999)** When this timer expires and the Switch has not observed (snooped) any IGMP query packets asking whether any stations belong to any Multicast groups, the Switch itself will send out queries and become the IGMP host on your network.
- **IP Multicast Filtering (IGMP Snooping)** This enables or disables the Switch to intelligently forward IGMP and Multicast packets instead of broadcasting (flooding) them on all ports. This setting also enables IGMP Snooping, which enables the Switch to read IGMP packets being forwarded through the Switch in order to obtain forwarding information from them (learn which ports contain Multicast members).

If *IEEE 802.1Q VLANs* is selected on the **VLANs & MAC-based Broadcast Domains Configuration** screen, **Configure 802.1Q IGMP** will appear at the bottom of the **IGMP Configuration** screen. This screen allows IGMP to operate in conjunction with IEEE 802.1Q VLANs. The screen is shown below:

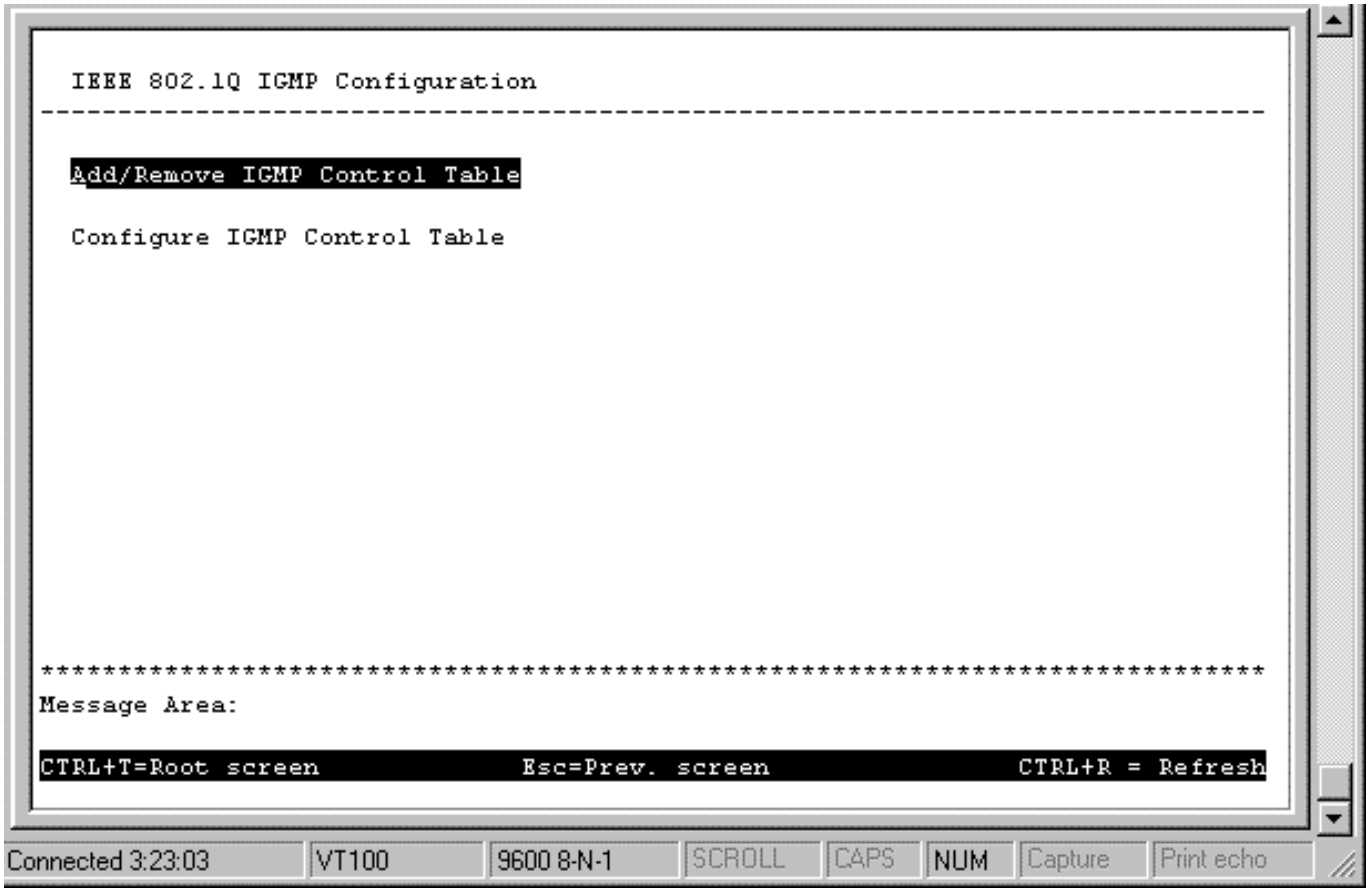


Figure 6-24. IEEE 802.1Q IGMP Configuration screen

Choosing **Add/Remove IGMP Control Table** allows you to define up to 12 VLANs on the Switch which can send and receive IGMP packets. Choosing **Configure IGMP Control Table** allows you to enable or disable these agents, and set aging timers for them. Both screens are shown below:

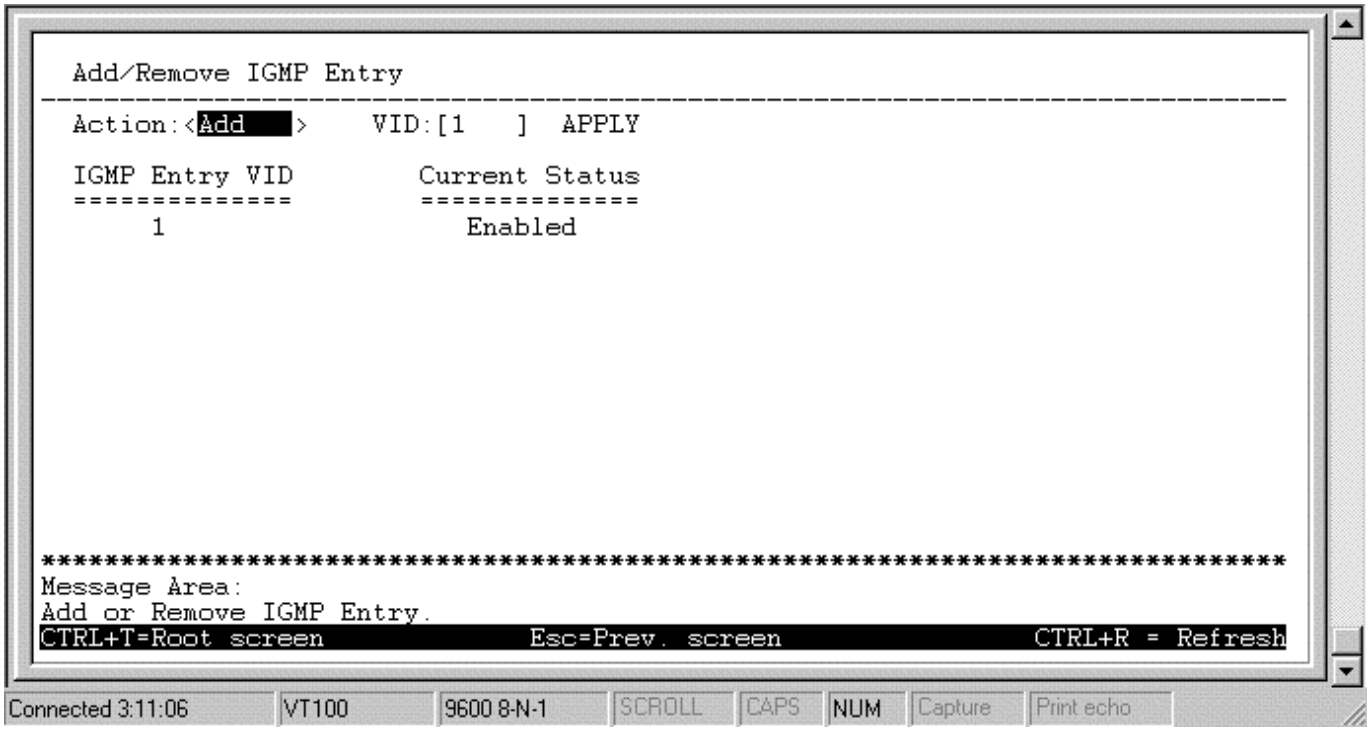


Figure 6-25. Add/Remove IGMP Entry screen

The above screen is used to specify an agent to interface between IGMP and VLAN. The agents are assigned to a VLAN and allow IGMP query and report packets to be present on the given VLAN. Only 12 agents can exist on the Switch at any one time.

Items in the above screen are described below:

- **Action** Adds/Removes an entry (agent) from the table.
- **VID** The VLAN number that you wish to create an agent for.

Go back to the **Configure 802.1Q IGMP** screen and choose **Configure IGMP Control Table** (shown below) in order to activate or deactivate the agents and configure settings for them.

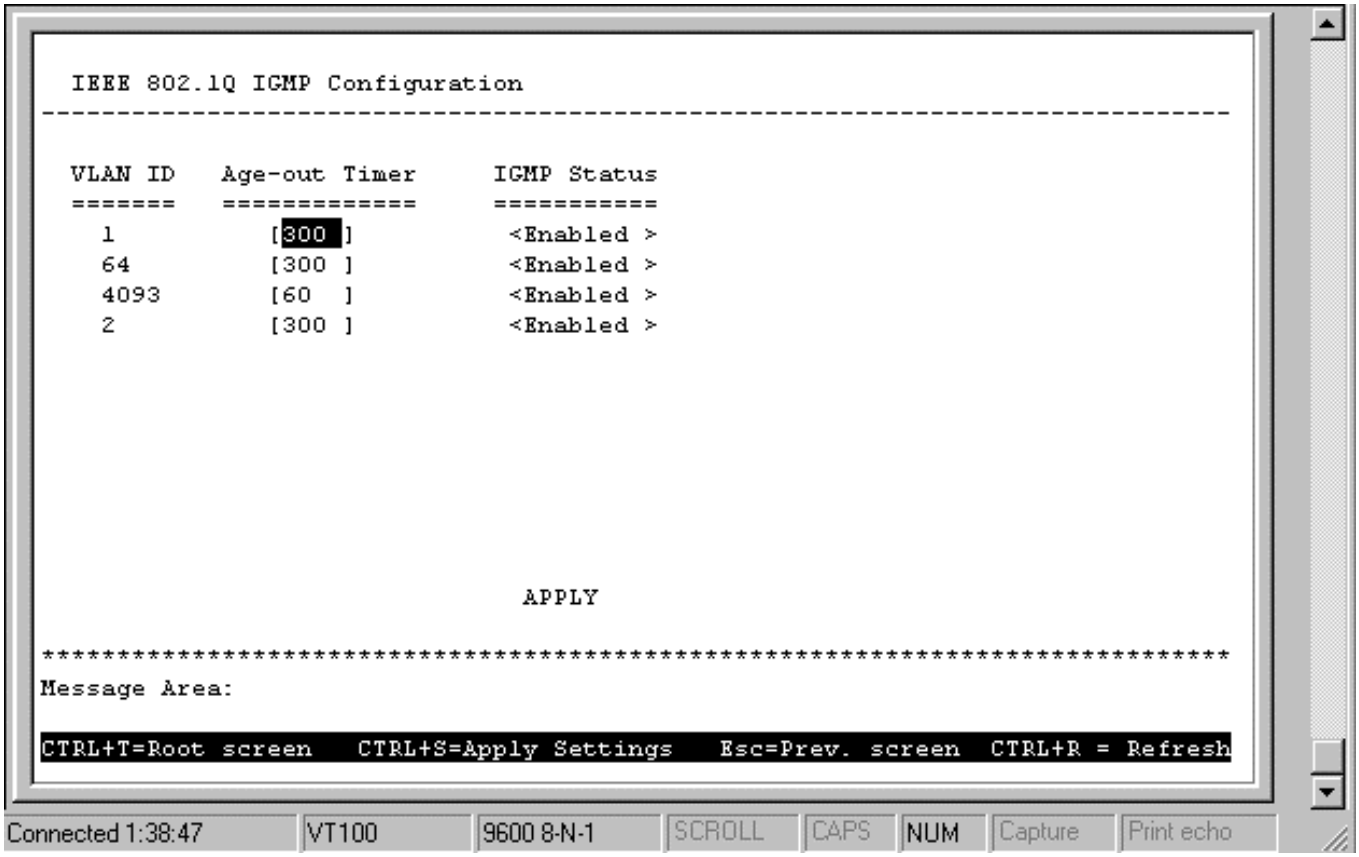


Figure 6-26. IEEE 802.1Q IGMP Configuration screen

Items in the above screen are defined as follows:

- **VLAN ID** This is the VID number for the VLAN that has an agent attached to it which enables IGMP packets to be sent and received.
- **Age-out Timer** If no IGMP query packet has arrived at the Switch before this timer has expired, the Switch will become the IGMP host for this VLAN.
- **IGMP Status** Activates/deactivates the agent on this VLAN.

Configure VLANs & MAC-based Broadcast Domains

If you are unsure about your knowledge of VLANs and broadcast domains, please review the *VLANs and Broadcast Domains* section in the *"Switch Management Concepts"* chapter of this manual before configuring the switch.

The **VLANs & MAC-based Broadcast Domains Configuration** menu displays the status of the current VLAN mode and allows a user to restart the Switch in a particular VLAN mode – *Port-Based VLANs*, *IEEE 802.1Q VLANs,* or *MAC-based Broadcast Domains* – or to choose *None*. There are four different versions of the **VLANs & MAC-based Broadcast Domains Configuration** menu, depending on which of the options you select under the Restart Mode (three of the four are displayed and explained below—the menu for *None* is omitted as it does not contain additional menu items at the bottom of the screen). Please note that the Switch can only support a single type of mode at any given time.

To view the **VLANs & MAC-based Broadcast Domains Configuration** menu for MAC-based Broadcast Domains:

1. Choose **Configure VLANs & MAC-based Broadcast Domains** on the **Configuration** menu.

2. Select *MAC-based Broadcast Domains* under Restart Mode and then press APPLY.

3. Press RESTART on the **Change VLAN Mode** screen (pictured below). This will cause the Switch to automatically save changes and then perform a reboot.

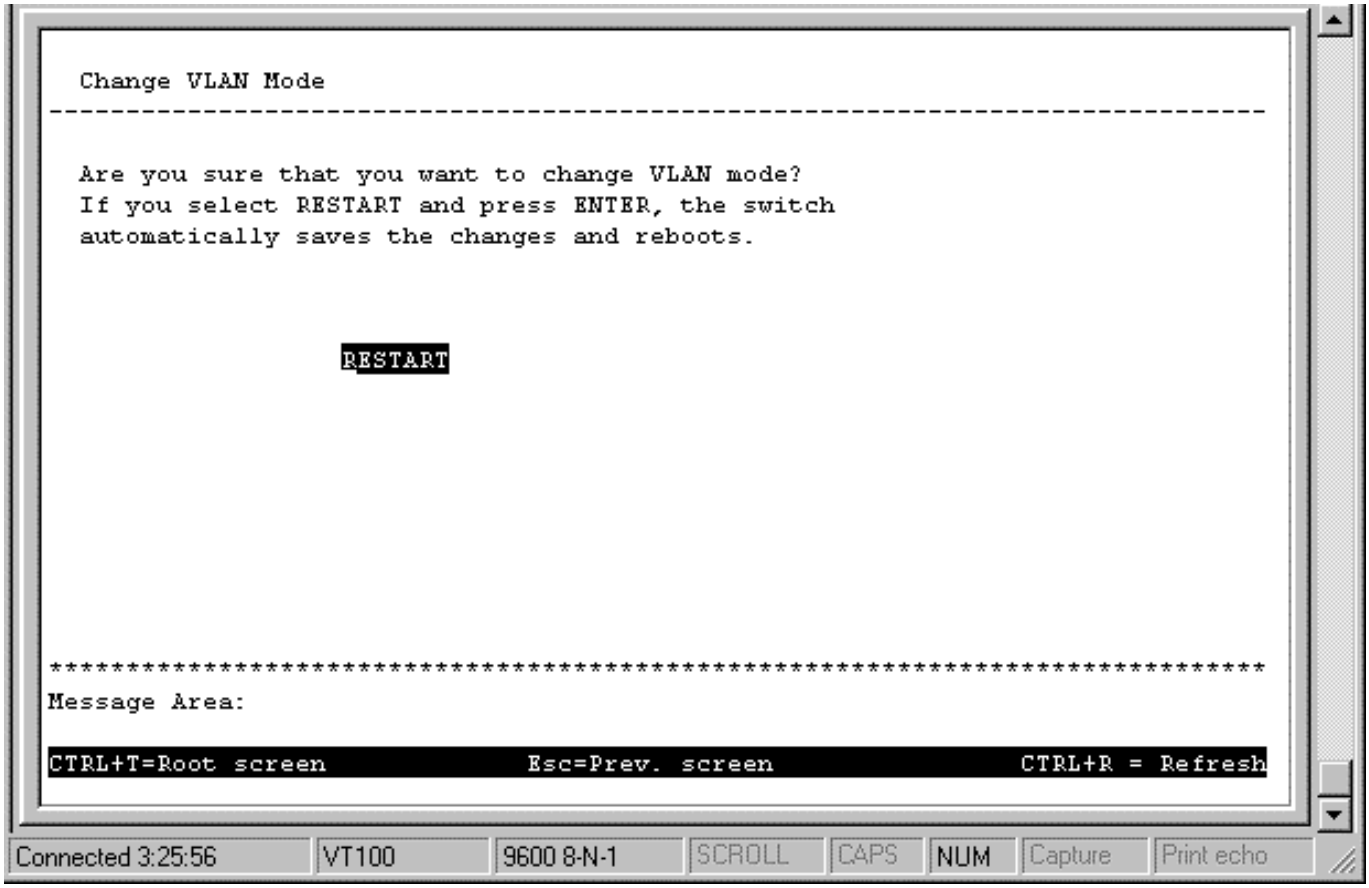


Figure 6-27. Change VLAN Mode screen

4. Repeat the first step. The following screen will appear:

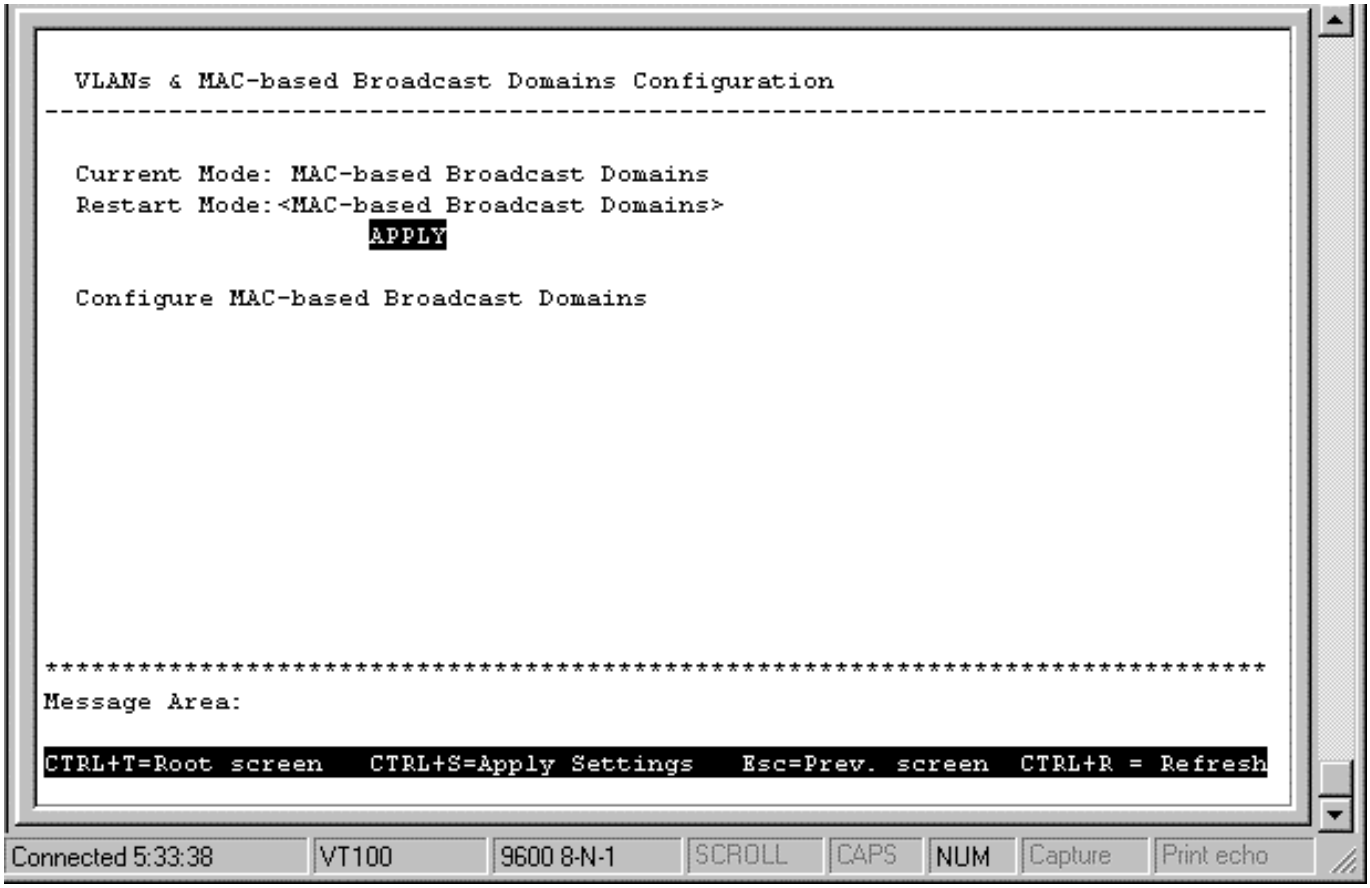


Figure 6-28. VLANs & MAC-based Broadcast Domains Configuration menu for MAC-based Broadcast Domains

The information on the top of the screen is described as follows:

- **Current Mode** Either displays the current VLAN or MAC-based Broadcast Domain mode or *None*.
- **Restart Mode** Choose from four settings: *MAC-based Broadcast Domains* (pictured above), *IEEE 802.1Q VLANs*, *Port-Based VLANs*, or *None*.

Configure MAC-based Broadcast Domains

To create a MAC-based Broadcast Domain, simply create the Broadcast Domain itself in the **Add/Remove MAC-based Broadcast Domains** screen by selecting *Add* in the Action field, entering a name in the Domain Name field, and then pressing APPLY). Next, select the Broadcast Domain you have created in the **Add/Remove MAC-based Broadcast Domain Members** screen. Finally, assign MAC addresses for each Broadcast Domain member you want to add in the **Add/Remove MAC-based Broadcast Domain Members** screen--select *Add* in the Action field, enter a MAC Address in the next field, and then press APPLY. Note that once all additions and changes have been completed, you must restart the Switch for the MAC-based Broadcast Domains to be implemented.

To access the **MAC-based Broadcast Domains Configuration** menu, open **Configuration**, choose **Configure VLANs & MAC-based Broadcast Domains**, and select **Configure MAC-based Broadcast Domains** at the bottom of the **VLANs & MAC-based Broadcast Domains Configuration** menu (the Current Mode must be *MAC-based Broadcast Domains*). The following menu appears:

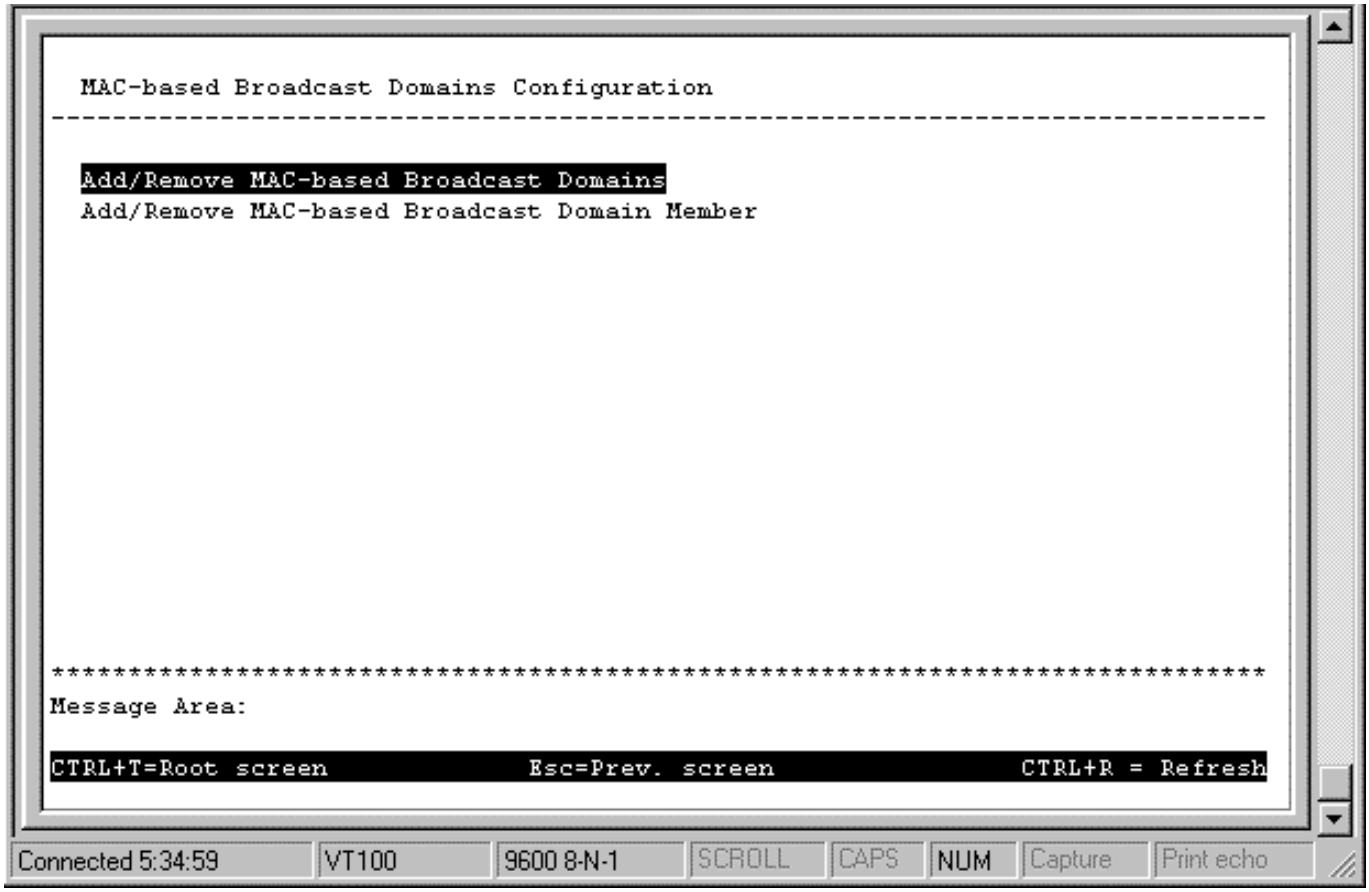


Figure 6-29. MAC-based Broadcast Domains Configuration menu

Choose **Add/Remove MAC-based Broadcast Domain** to access the following screen:

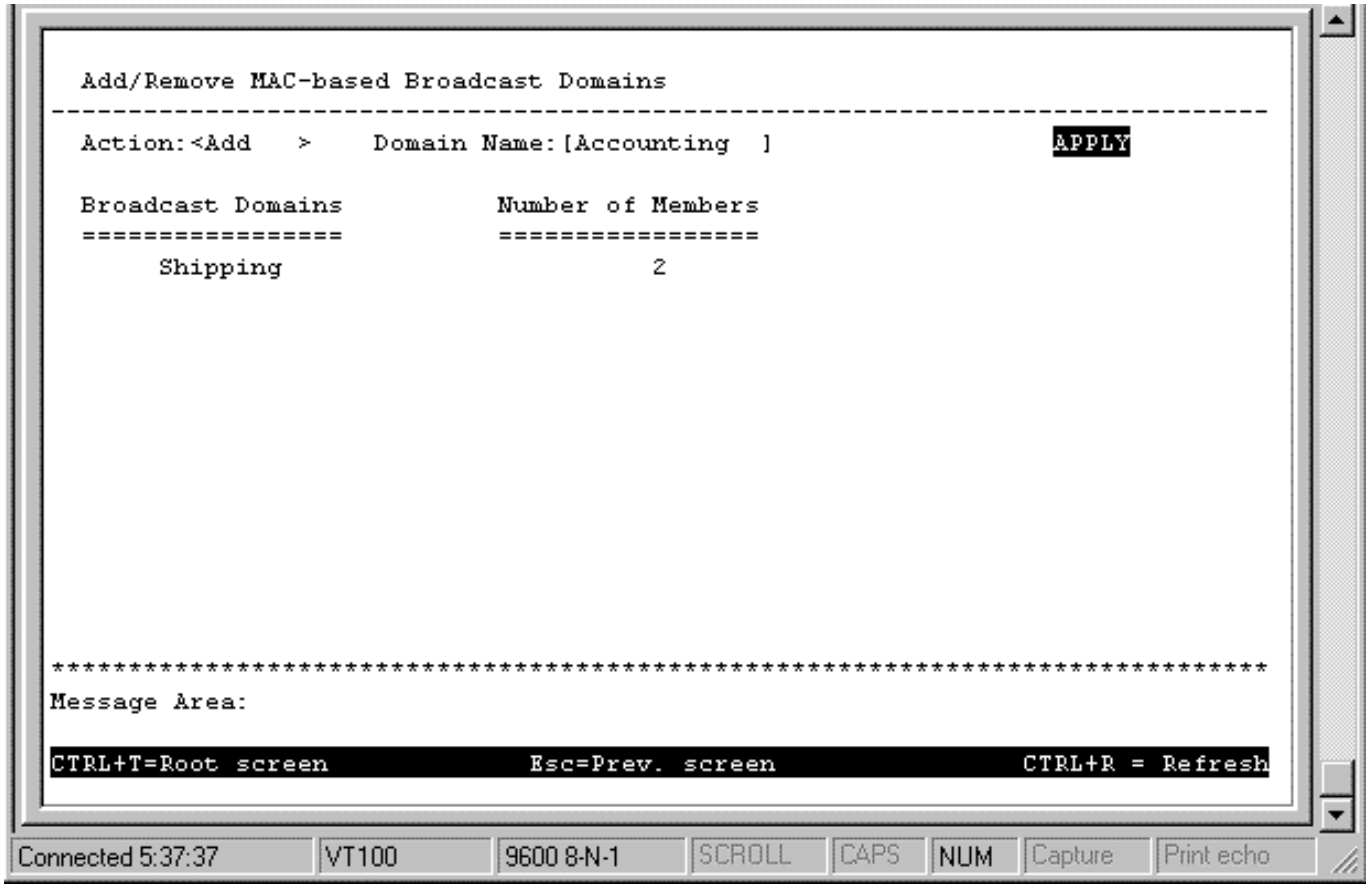


Figure 6-30. Add/Remove MAC-based Broadcast Domains screen

The fields you can set are:

- **Action** *Add* or *Remove* a MAC-based Broadcast Domain.
- **Domain Name** Enter the name of the MAC-based Broadcast Domain.

Press APPLY to create or remove the designated MAC-based Broadcast Domain.

Broadcast Domains and **Number of Members** reflect the current conditions. They are read-only fields and cannot be changed.

Choose **Add/Remove MAC-based Broadcast Domain Member** from the **MAC-based Broadcast Domains Configuration** menu to access the following screen:

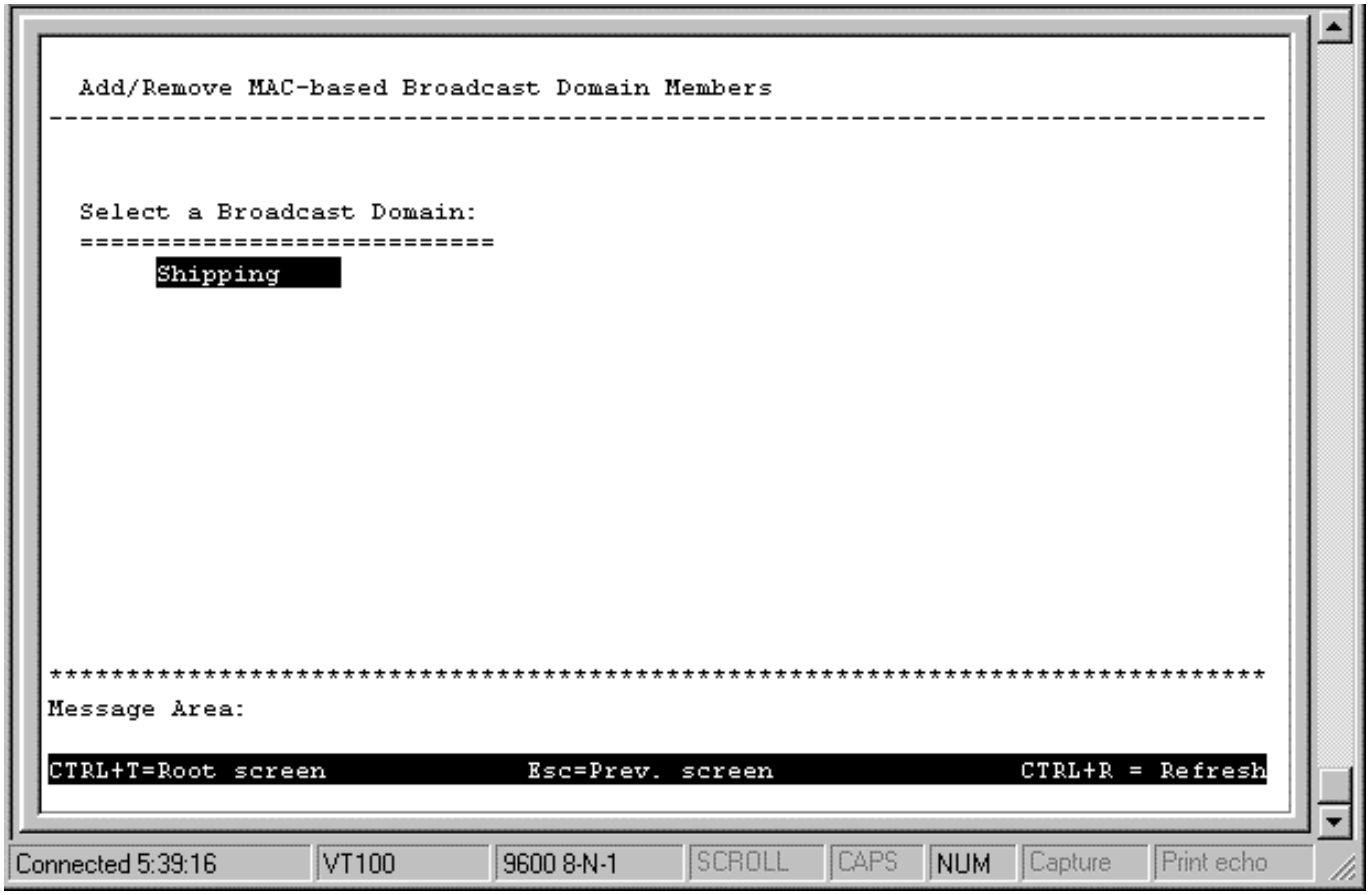


Figure 6-31. the first Add/Remove MAC-based Broadcast Domain Members screen

To configure a MAC-based Broadcast Domain member, highlight the desired entry on the screen above and press <Enter>. The following screen appears:

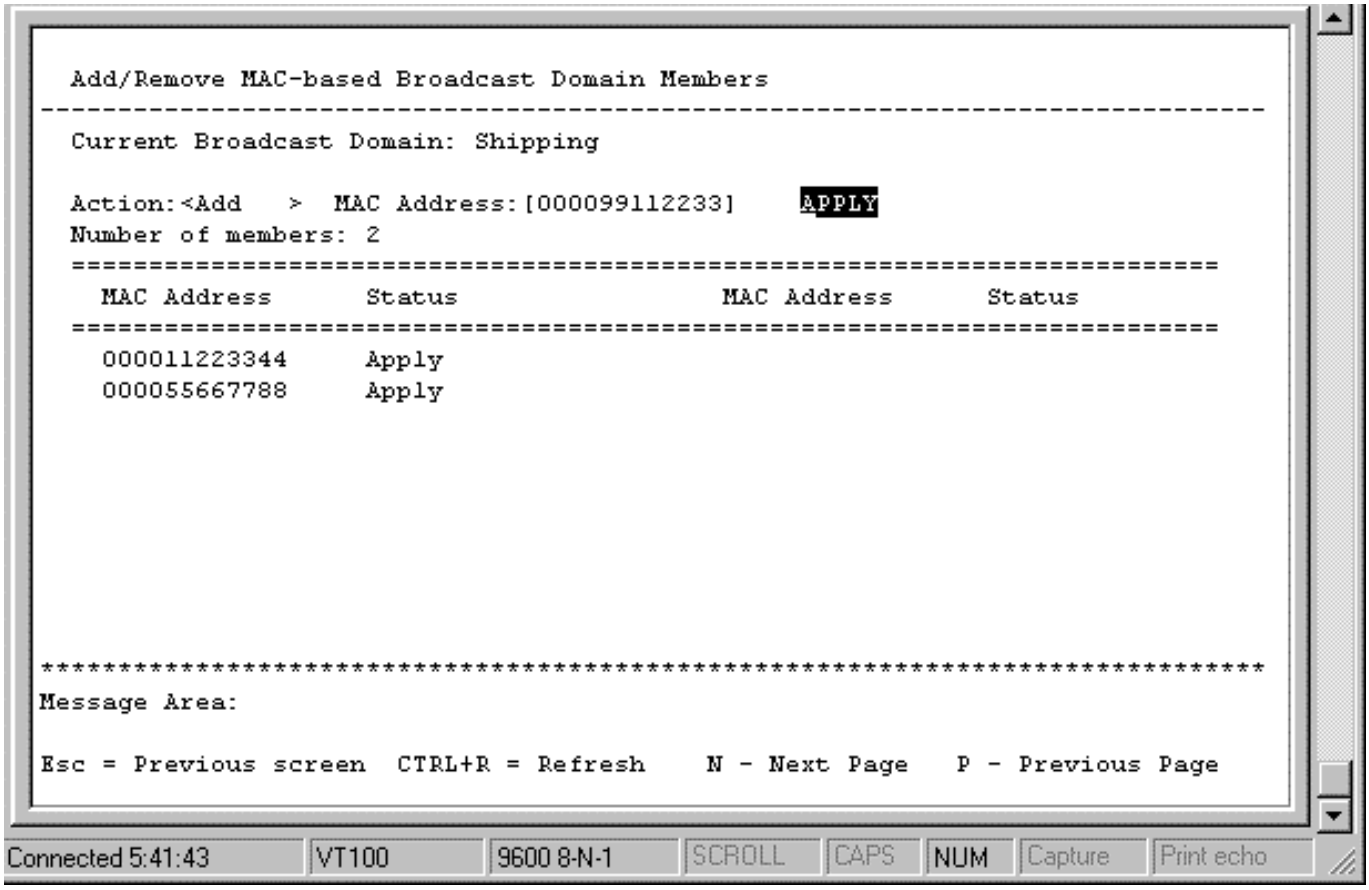


Figure 6-32. the second Add/Remove MAC-based Broadcast Domain Members screen

The fields you can set are:

- **Action** Select the desired action by toggling between *Add* and *Remove*.
- **MAC Address** The MAC address of the Broadcast Domain member being added or removed.

Please note that the Status field for the MAC address you have entered will read *Not Apply* if it is the same MAC address entered in the filtering and forwarding table..

Current Broadcast Domain, **Number of members**, **MAC Address** (in the lower part of the screen), and **Status** reflect the current conditions. They are read-only fields and cannot be changed.

Configure Port-based VLAN

If you are unsure of your knowledge of port-based VLANs, we highly recommend reviewing the *VLANs and Broadcast Domains* section of the *"Switch Management Concepts"* chapter in this manual before proceeding.

To view the **VLANs & MAC-based Broadcast Domains Configuration** menu for Port-based VLANs:

1. Choose **Configure VLANs & MAC-based Broadcast Domains** on the **Configuration** menu.
2. Select *Port-Based VLANs* under Restart Mode and then press APPLY.
3. Press RESTART on the **Change VLAN Mode** screen. This will cause the Switch to automatically save changes and then perform a reboot.
4. Repeat the first step. The following screen will appear:

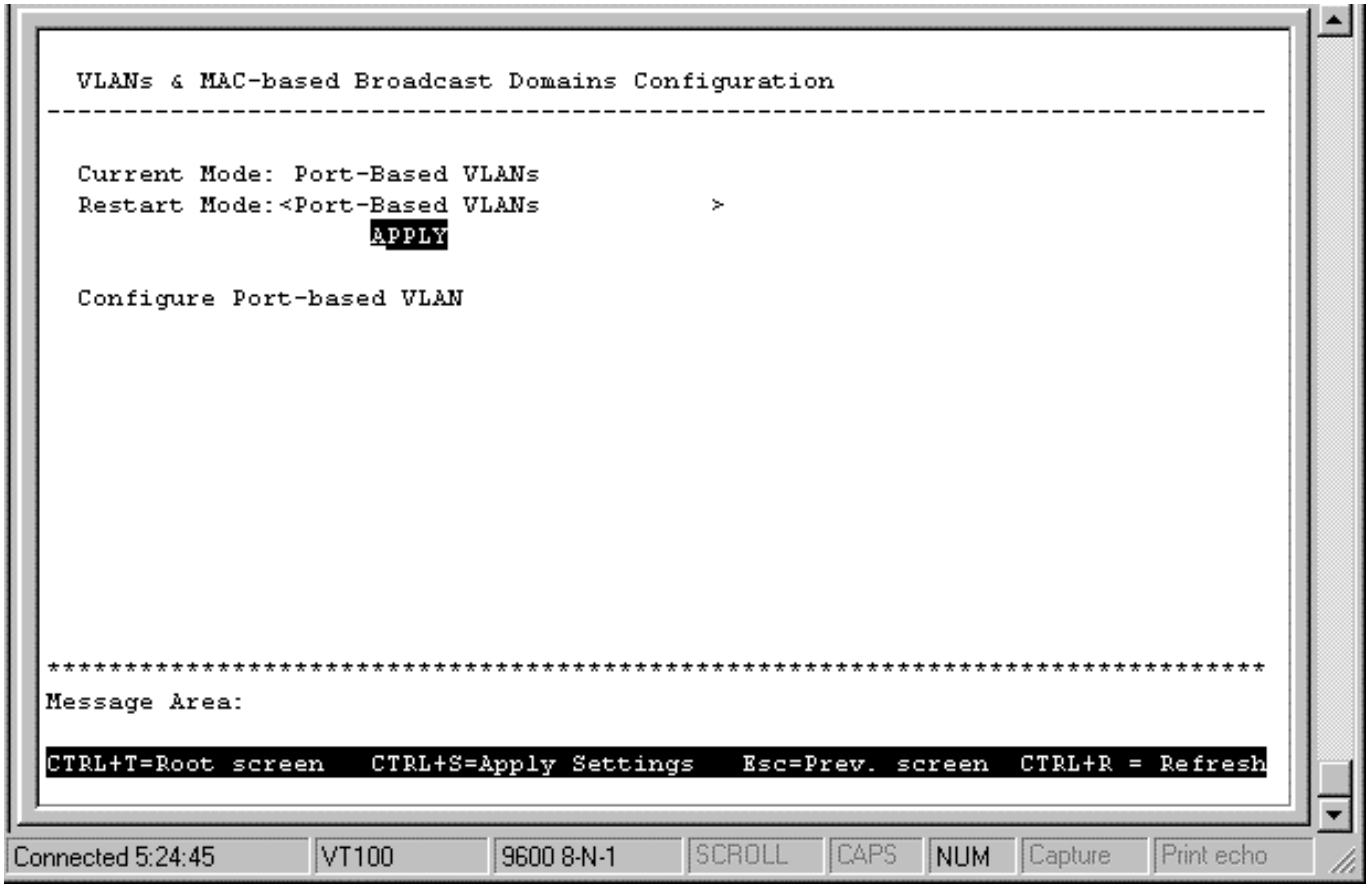


Figure 6-33. VLANs & MAC-based Broadcast Domains Configuration menu for Port-Based VLANs

Choose **Configure Port-Based VLAN** on the screen above to access the **Configure VLAN (Port-Based)** menu:

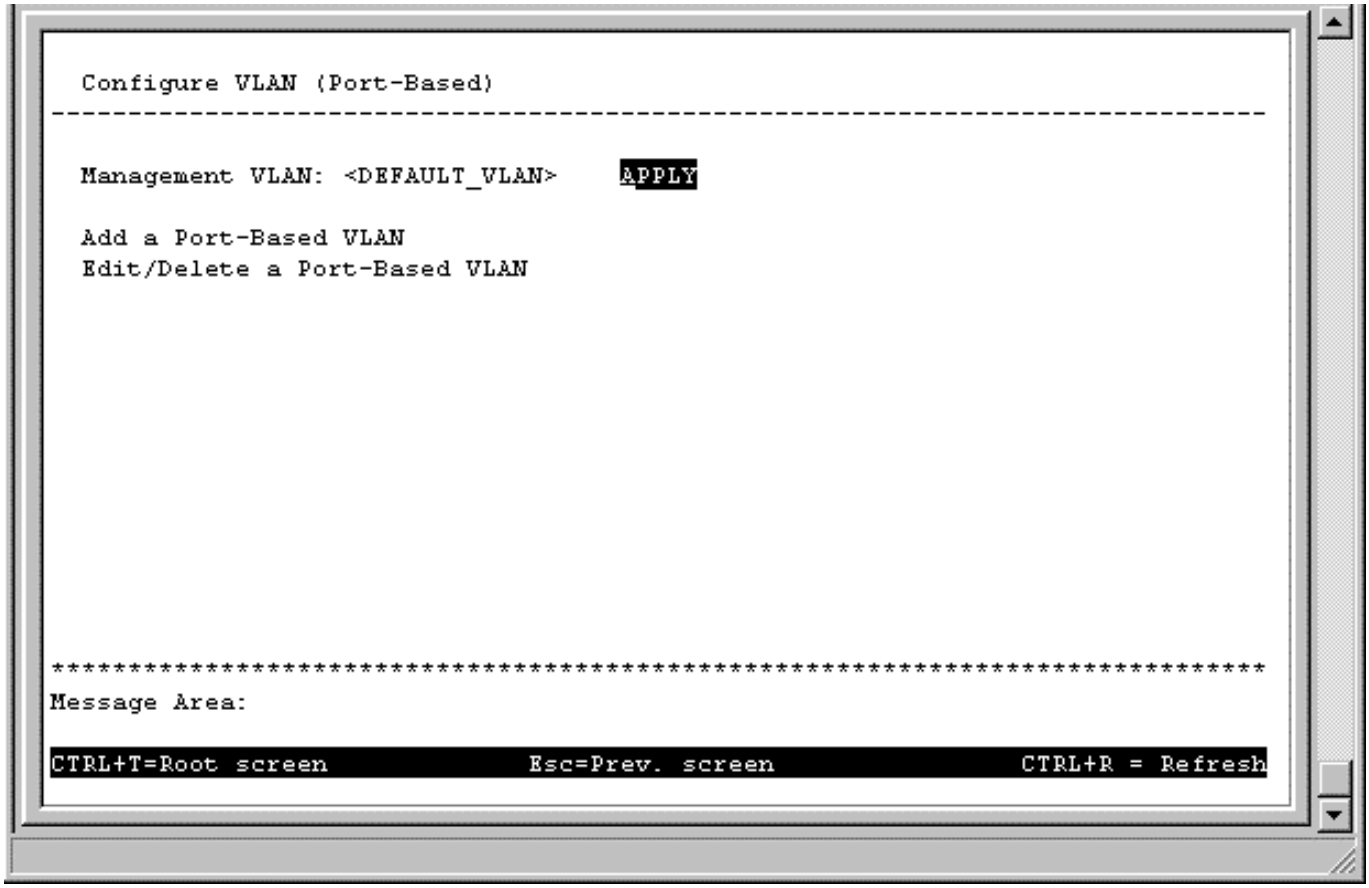


Figure 6-34. Configure VLAN (Port-Based) menu

To create a Port-based VLAN, select **Add a Port-Based VLAN** on the screen above and then press APPLY. The following screen appears:

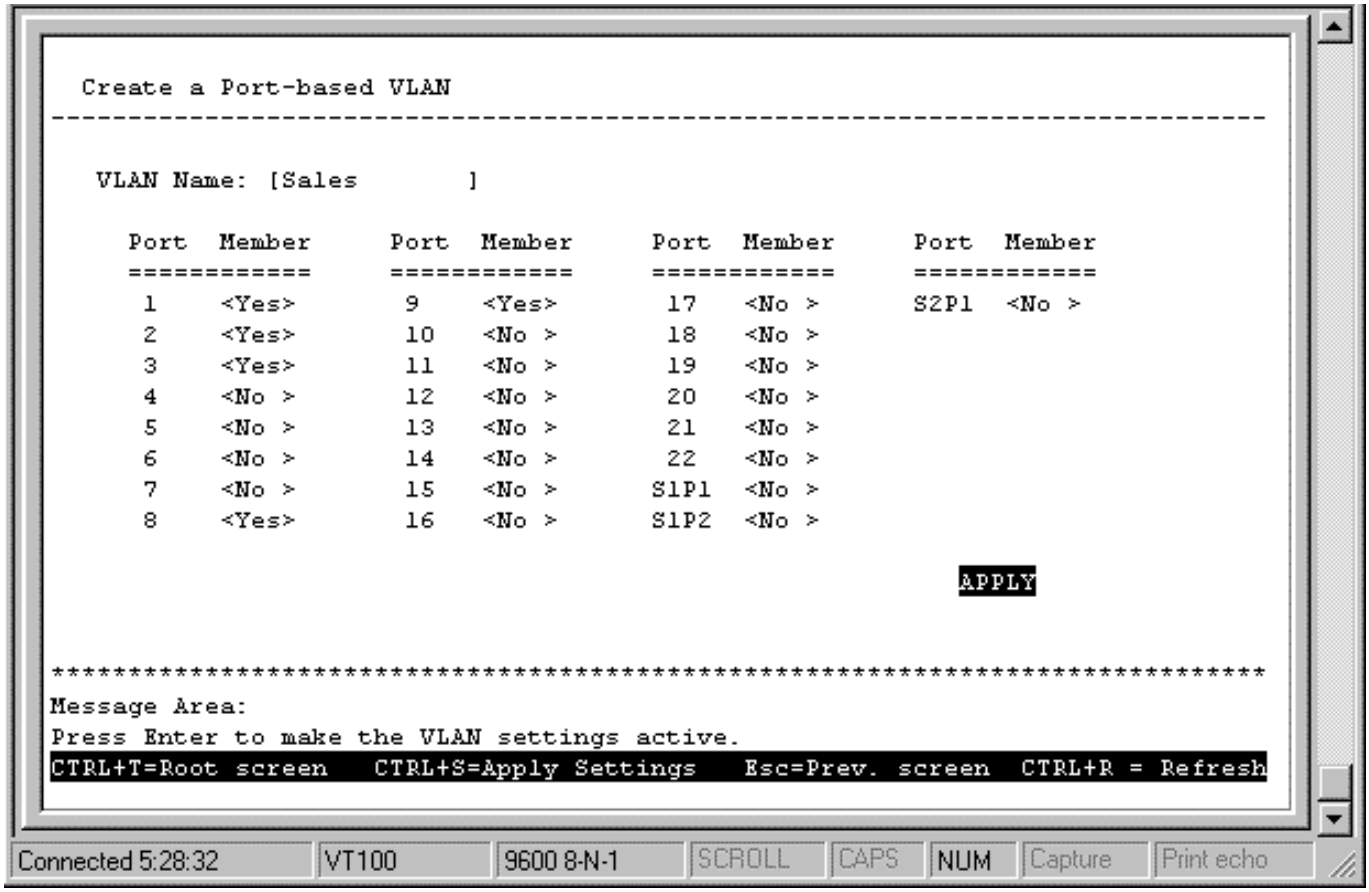


Figure 6-35. Create a Port-based VLAN screen

Enter a name for your new VLAN in the VLAN Name field at the top of the screen above. Next, select which ports will become members of the VLAN by toggling between *Yes* and *No* in the Member column. Click APPLY to let the changes immediately take effect.

To modify or delete a Port-based VLAN, select **Edit/Delete a Port-Based VLAN** on the screen above and then press APPLY. The following screen appears:

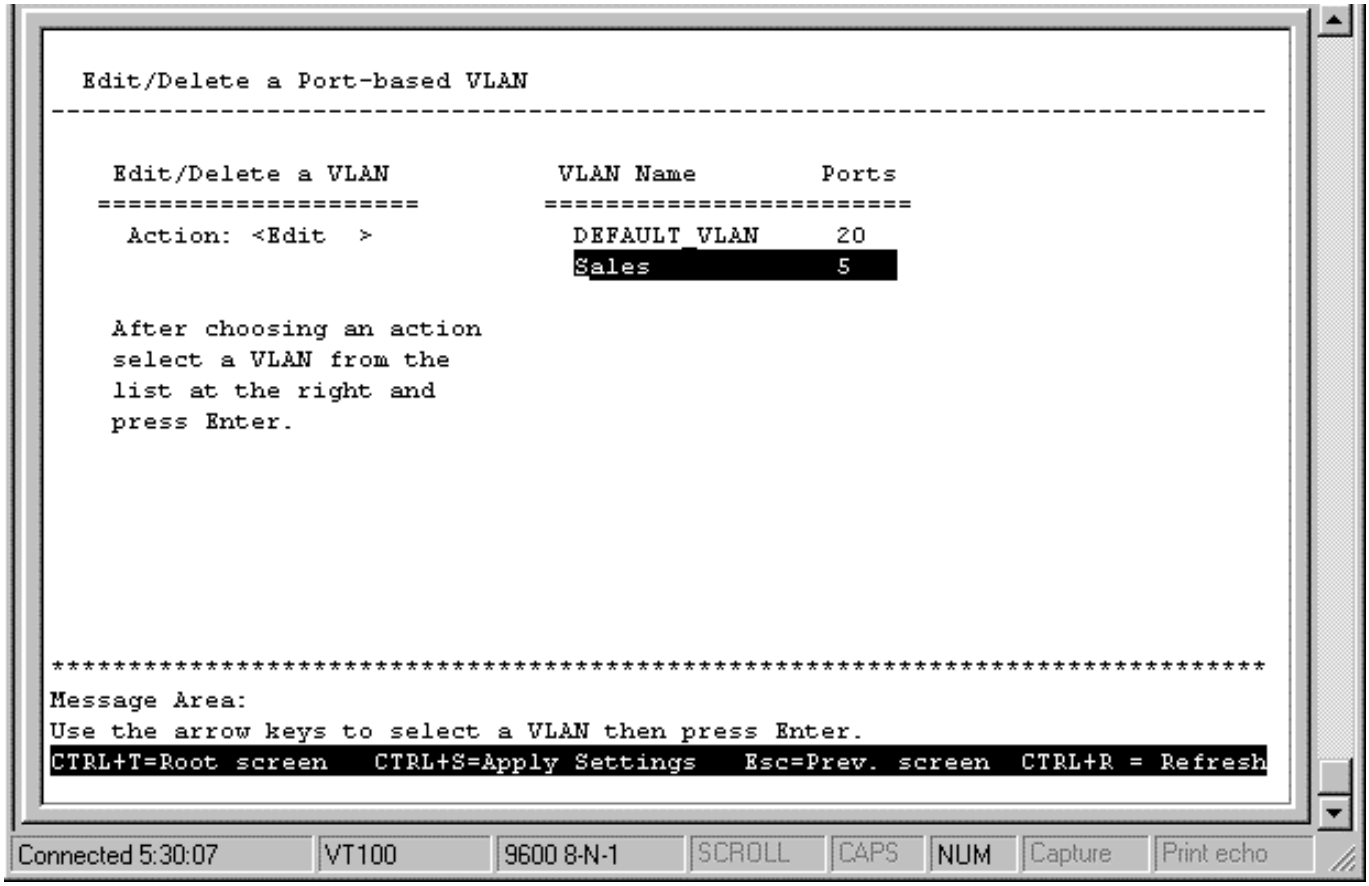


Figure 6-36. Edit/Delete a Port-based VLAN screen

After selecting *Edit* or *Delete* in the Action field, choose a VLAN from the list on the right-side of the screen above and then press <Enter>.

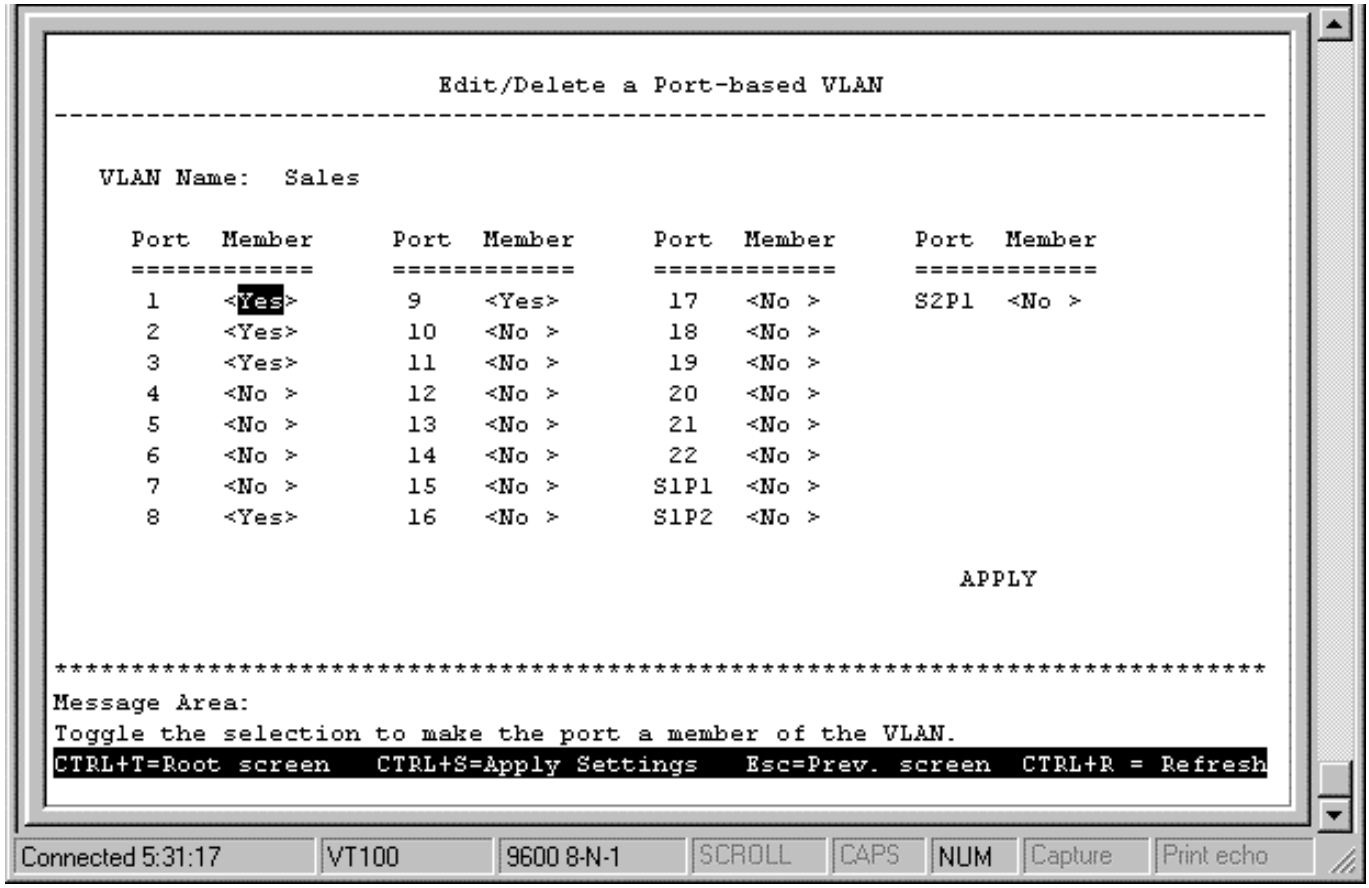


Figure 6-37. Edit/Delete a Port-based VLAN table

Use this screen to either add or drop a member from a specified VLAN. Press APPLY when finished with all your changes.

Configure IEEE 802.1Q VLANs

To configure an IEEE 802.1 port-based VLAN, you must do three things:

1. Decide if you want to enable Ingress Filtering and enable it on the chosen ports. Ingress filtering applied on a port causes the port to examine all incoming packets and check whether the port itself is a member of the VLAN. This is normally used to keep untagged frames off the Switch, although it can have other uses as well. This setting is configurable for each port in the **Configure Port Ingress Filter** screen.

2. Define which ports will be active members of the VLAN. A port can transmit packets onto only one VLAN. It can receive packets (be a passive member) on many VLANs. Active VLANs are designations are defined by assigning Port VLAN ID numbers (PVIDs) in the **Configure Port VLAN ID** screen.

3. Define the VLAN itself and which ports will be members (able to receive packets from a port that has this PVID number). At this point, you need to designate whether a member port will be a Tagging or Untagging member port. Defining the ports that will be members of a VLAN, and whether they will Tag or Untag packets is done in the **Configure Static VLAN Entry** screen.

4. Determine whether to enable GARP VLAN Registration Protocol (GVRP) in order to update dynamic registration entries as well as to communicate information to other VLAN-aware workstations and bridges, thus allowing orders to issue and revoke VLAN membership. GVRP can be enabled for individual ports on the **GVRP Configuration** screen.

To view the **VLANs & MAC-based Broadcast Domains Configuration** menu for MAC-based Broadcast Domains:

1. Choose **Configure VLANs & MAC-based Broadcast Domains** on the **Configuration** menu.
2. Select *IEEE 802.1Q VLANs* under Restart Mode and then press APPLY.
3. Press RESTART on the **Change VLAN Mode** screen. This will cause the Switch to automatically save changes and then perform a reboot.
4. Repeat the first step. The following screen will appear:

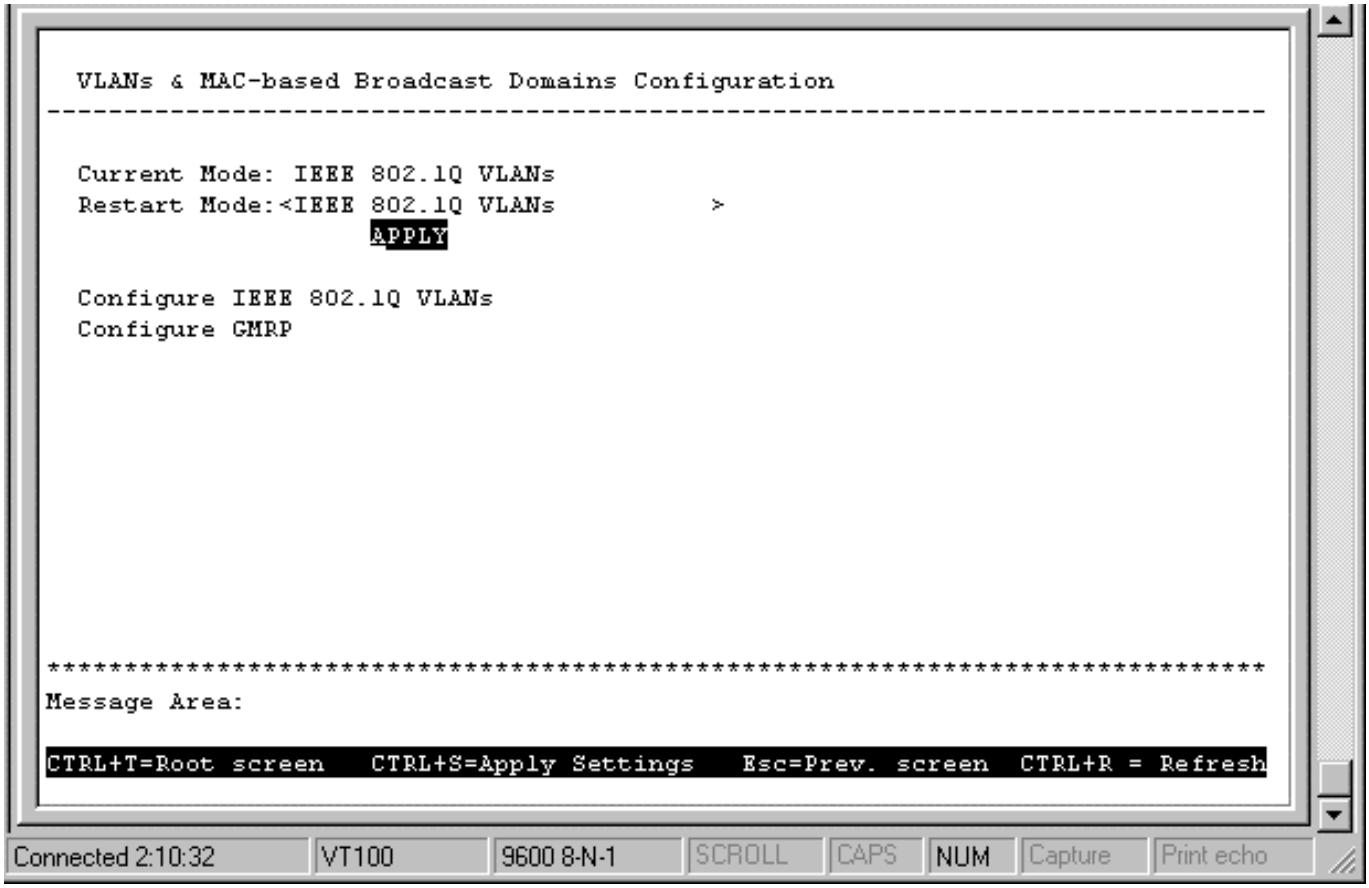


Figure 6-38. VLANs & MAC-based Broadcast Domains Configuration menu for IEEE 802.1Q VLANs

Choose **Configure IEEE 802.1Q VLANs** on the screen above (under **Configure VLANs & MAC-based Broadcast Domains** of the **Configuration** menu) to access the **IEEE 802.1Q VLANs Configuration** menu:

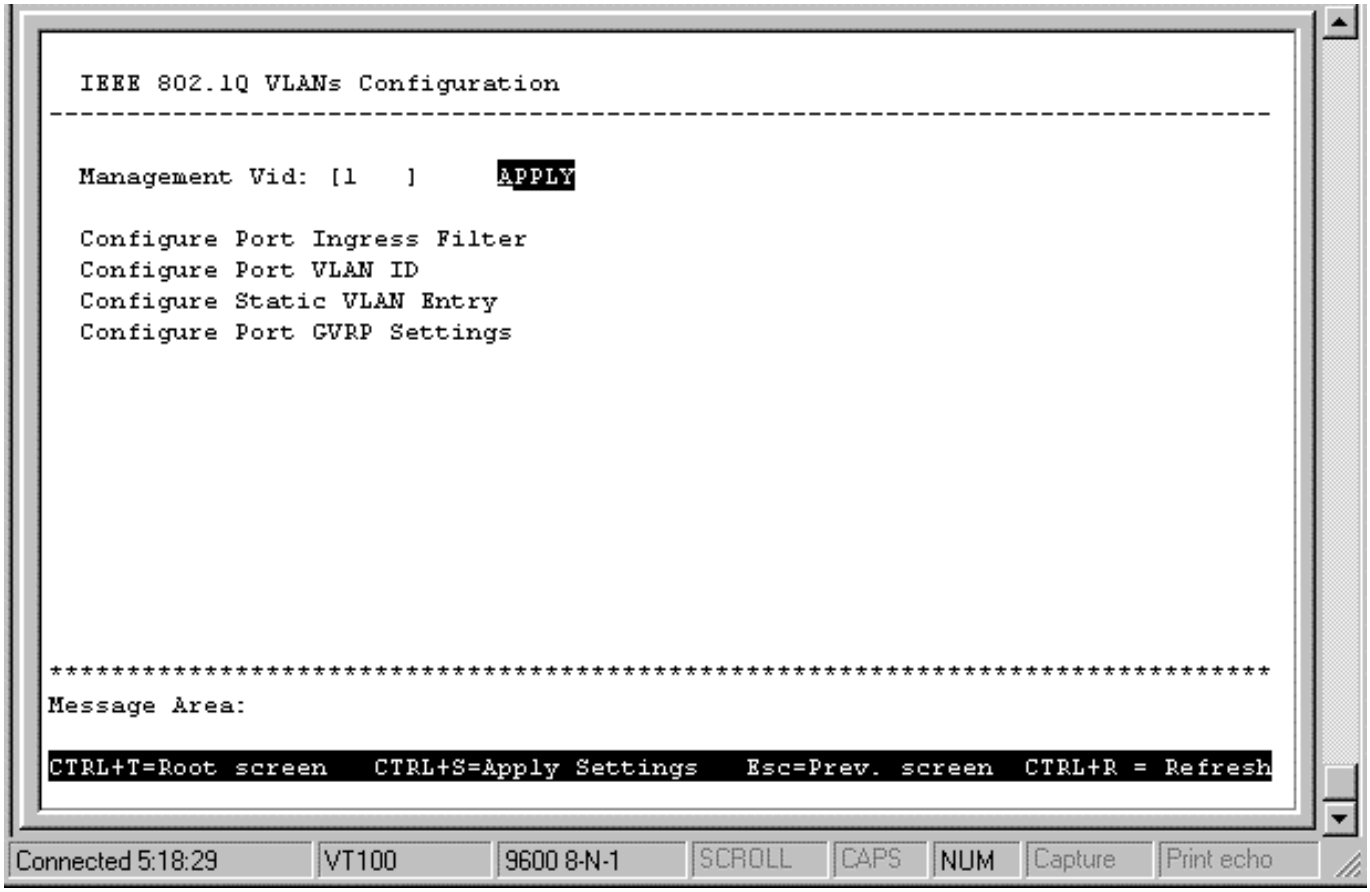


Figure 6-39. IEEE 802.1Q VLANs Configuration menu

Enter a Management VID in the first field and press APPLY to let the change take effect.

The field you can set is:

- **Management Vid** When *IEEE 802.1Q VLANs* are enabled, this is the VLAN that will be used for management packets. Make sure the Switch port that the management station is connected to has this PVID number and is a member of this 802.1Q VLAN (VID). This should be the first VLAN you create, otherwise, you may not be able to communicate with the Switch except through the console port.

Choose **Configure Port Ingress Filter** to access the first item on the menu. The following screen appears:

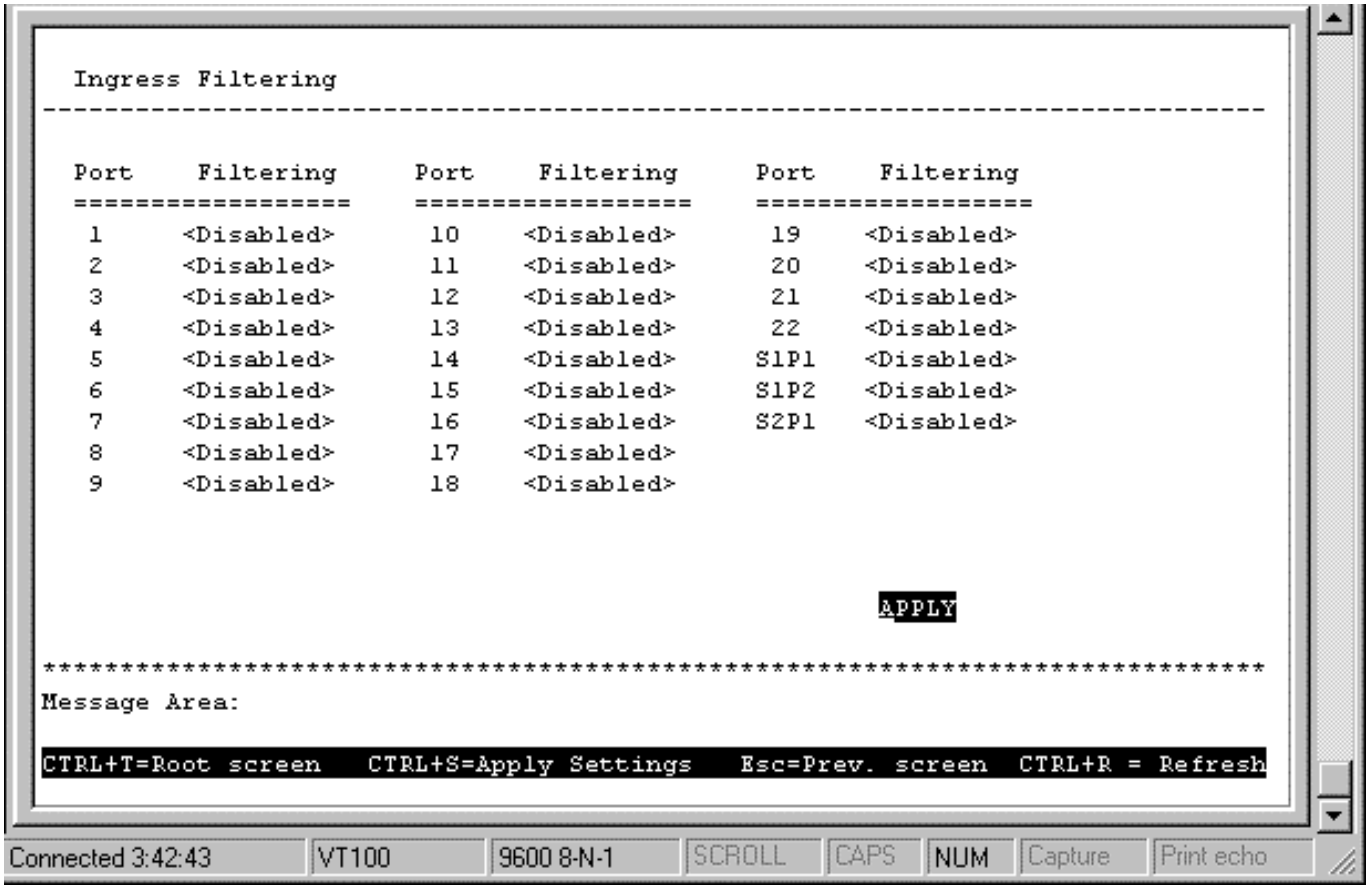


Figure 6-40. Ingress Filtering screen

This screen allows you to enable or disable Ingress filtering for each port. When a packet arrives at the port and Ingress filtering is *Enabled*, the port will check the VLAN ID number of the packet, and its own VIDs. If there is a match, the port will receive the packet. If the packet doesn't have a VLAN tag or the port is not a member of the VLAN for which the packet is tagged, the packet will be discarded.

Choose **Configure Port VLAN ID** to access the second item on the **IEEE 802.1Q VLANs Configuration** menu. The following **Port VLAN assignment** screen appears:

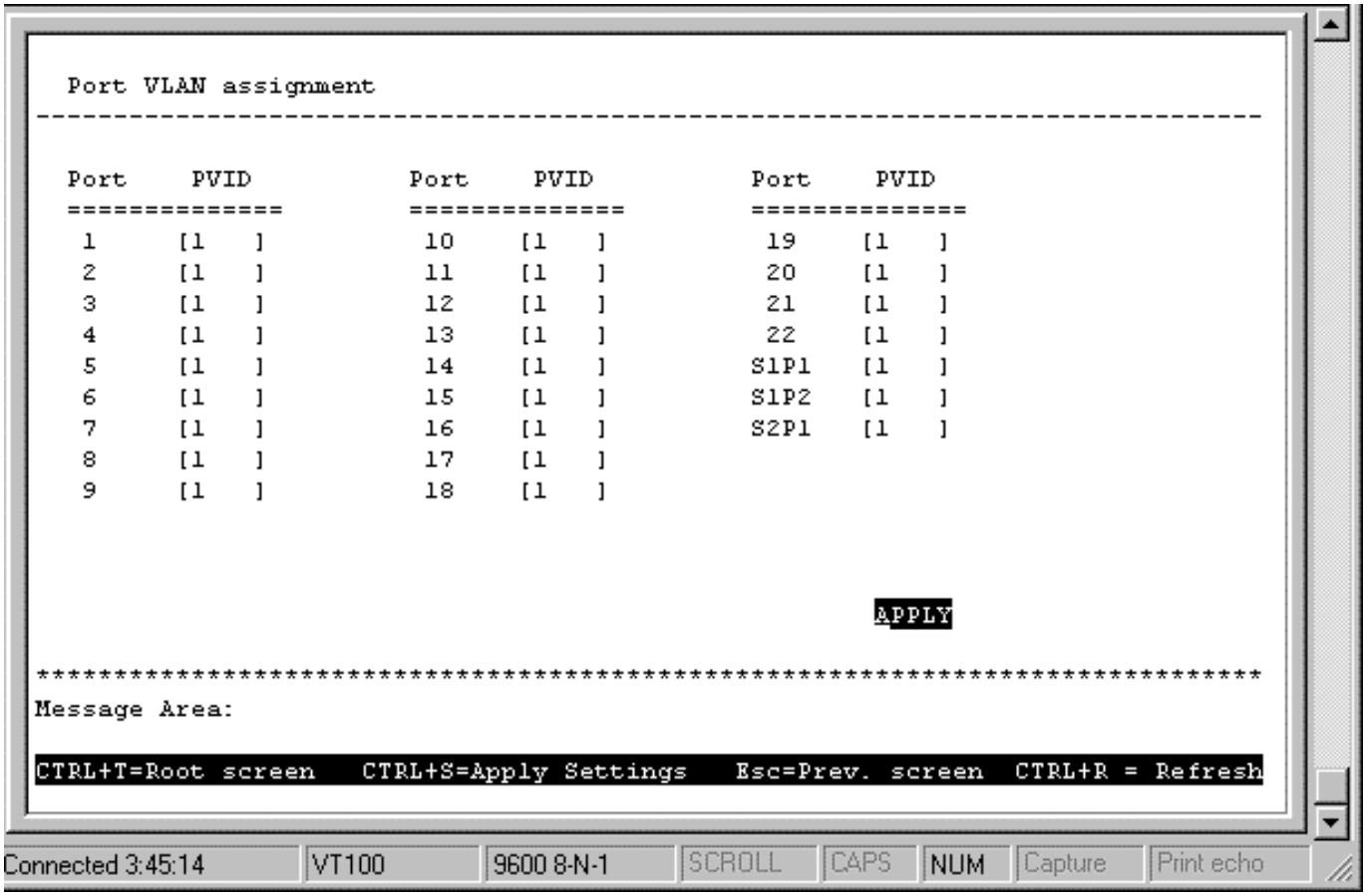

Port VLAN assignment
Port PVID Port PVID Port PVID
1 [1] 10 [1] 19 [1]
2 [1] 11 [1] 20 [1]
3 [1] 12 [1] 21 [1]
4 [1] 13 [1] 22 [1]
5 [1] 14 [1] S1P1 [1]
6 [1] 15 [1] S1P2 [1]
7 [1] 16 [1] S2P1 [1]
8 [1] 17 [1]
9 [1] 18 [1]
APPLY
Message Area:
CTRL+T=Root screen CTRL+S=Apply Settings Esc=Prev. screen CTRL+R = Refresh
Connected 3:45:14 VT100 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure 6-41. Port VLAN assignment screen

This screen allows you to set a Port VLAN ID number (PVID) for each port. Press APPLY to let the changes take effect.

Choose **Configure Static VLAN Entry** to access the third item on the **IEEE 802.1Q VLANs Configuration** menu. The following **802.1Q Static VLAN Settings** screen appears:

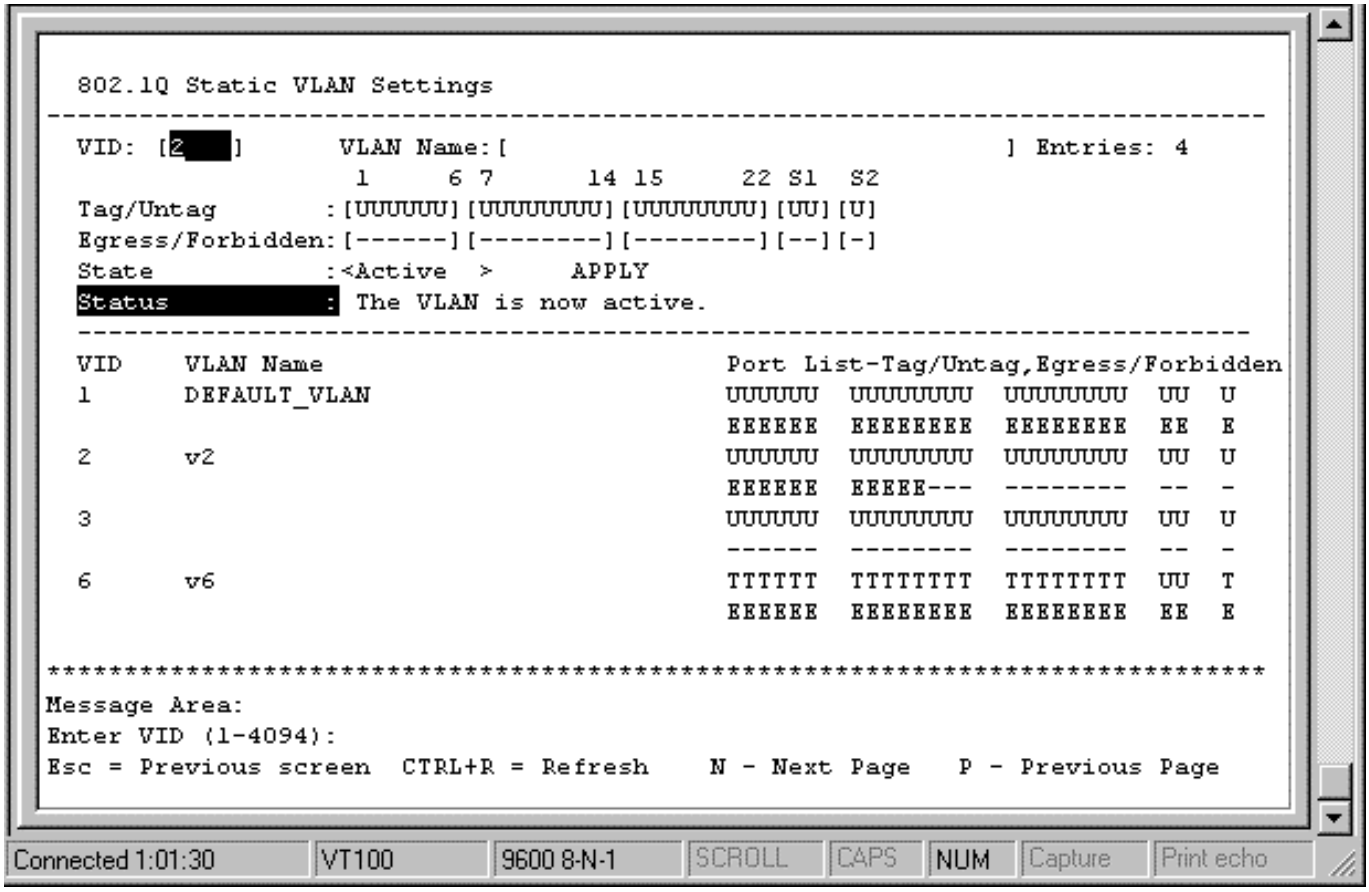

802.1Q Static VLAN Settings
VID: [2] VLAN Name:[ ] Entries: 4
1 6 7 14 15 22 S1 S2
Tag/Untag :[UUUUUU][UUUUUUUU][UUUUUUUU][UU][U]
Egress/Forbidden:[------][--------][--------][--][-]
State :<Active > APPLY
Status : The VLAN is now active.
VID VLAN Name Port List-Tag/Untag,Egress/Forbidden
1 DEFAULT_VLAN UUUUUU UUUUUUUU UUUUUUUU UU U
EEEEEE EEEEEEEE EEEEEEEE EE E
2 v2 UUUUUU UUUUUUUU UUUUUUUU UU U
EEEEEE EEEEE--- -------- -- -
3 UUUUUU UUUUUUUU UUUUUUUU UU U
------ -------- -------- -- -
6 v6 TTTTTT TTTTTTTT TTTTTTTT UU T
EEEEEE EEEEEEEE EEEEEEEE EE E
Message Area:
Enter VID (1-4094):
Esc = Previous screen CTRL+R = Refresh N - Next Page P - Previous Page
Connected 1:01:30
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 6-42. 802.1Q Static VLAN Settings screen

The fields you can set are:

- **VID** Enter a VLAN ID from 1 to 4094. This is the VLAN that will be defined on this screen.
- **VLAN Name** Description of the VLAN.
- **Tag/Untag** Toggle between *T* for tag and *U* for untag for each port.
- **Egress/Forbidden** Position the cursor over the dash "–" representing the appropriate port number and press <space bar> to select *E* for Egress, *F* for Forbidden or leave the dash "–". An *E* designates the specified port as a static member of the VLAN. An *F* defines the port as a non-member and also forbids the port from joining a VLAN dynamically. A dash (–) means the port is not given VLAN membership for the VID entered above.
- **State** Toggle between *Active* and *Inactive.*

A table on the lower part of the screen displays the settings for each VLAN. The table displays the VLAN number (**VID**), **VLAN Name**, and **Tag/Untag** and **Egress** (membership) status for all ports.

Choose **Configure Port GVRP Settings** to access the fourth item on the **IEEE 802.1Q VLANs Configuration** menu. The following **GVRP Configuration** screen appears:

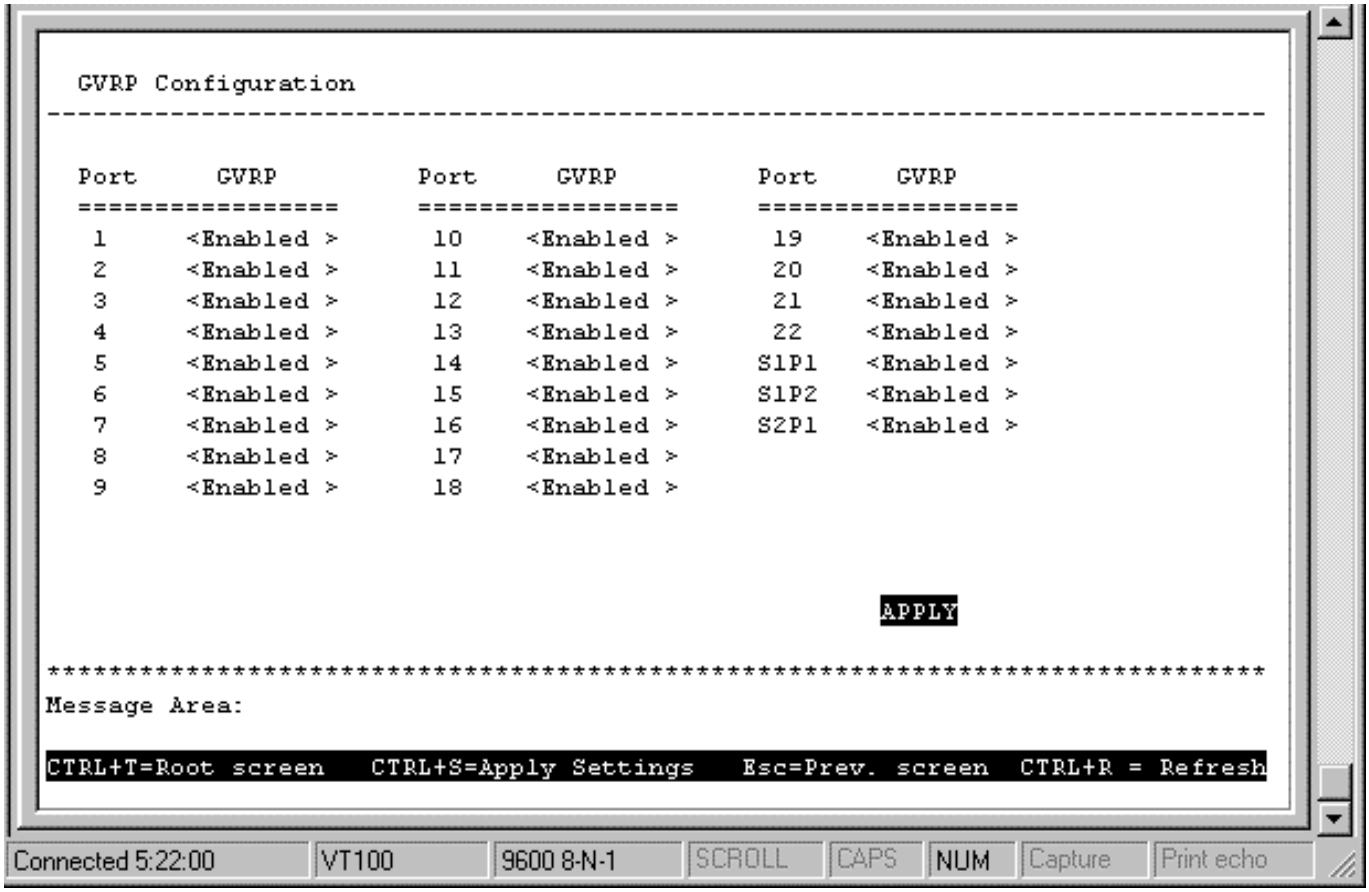


Figure 6-43. GVRP Configuration screen

This screen allows you to enable or disable GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol, on individual ports.

GVRP updates dynamic VLAN registration entries and communicates the new VLAN information across the network. This allows, among other things, for stations to physically move to other switch ports and keep their same VLAN settings, without having to reconfigure VLAN settings on the Switch.

Configure GMRP

Group Multicast Registration Protocol (GMRP) allows multicasts to be sent on a single VLAN without affecting other VLANs or broadcast domains. Group registration entries indicate for each port whether frames to be sent to a group MAC address and on a certain VLAN should be filtered or discarded. Use the **GMRP Configuration** screen to enable or disable GMRP.

Choose **Configure GMRP** from the bottom of the **VLANs & MAC-based Broadcast Domains Configuration** screen (the Switch must already be in *IEEE 802.1Q VLANs* mode) to access the following **GMRP Configuration** screen:

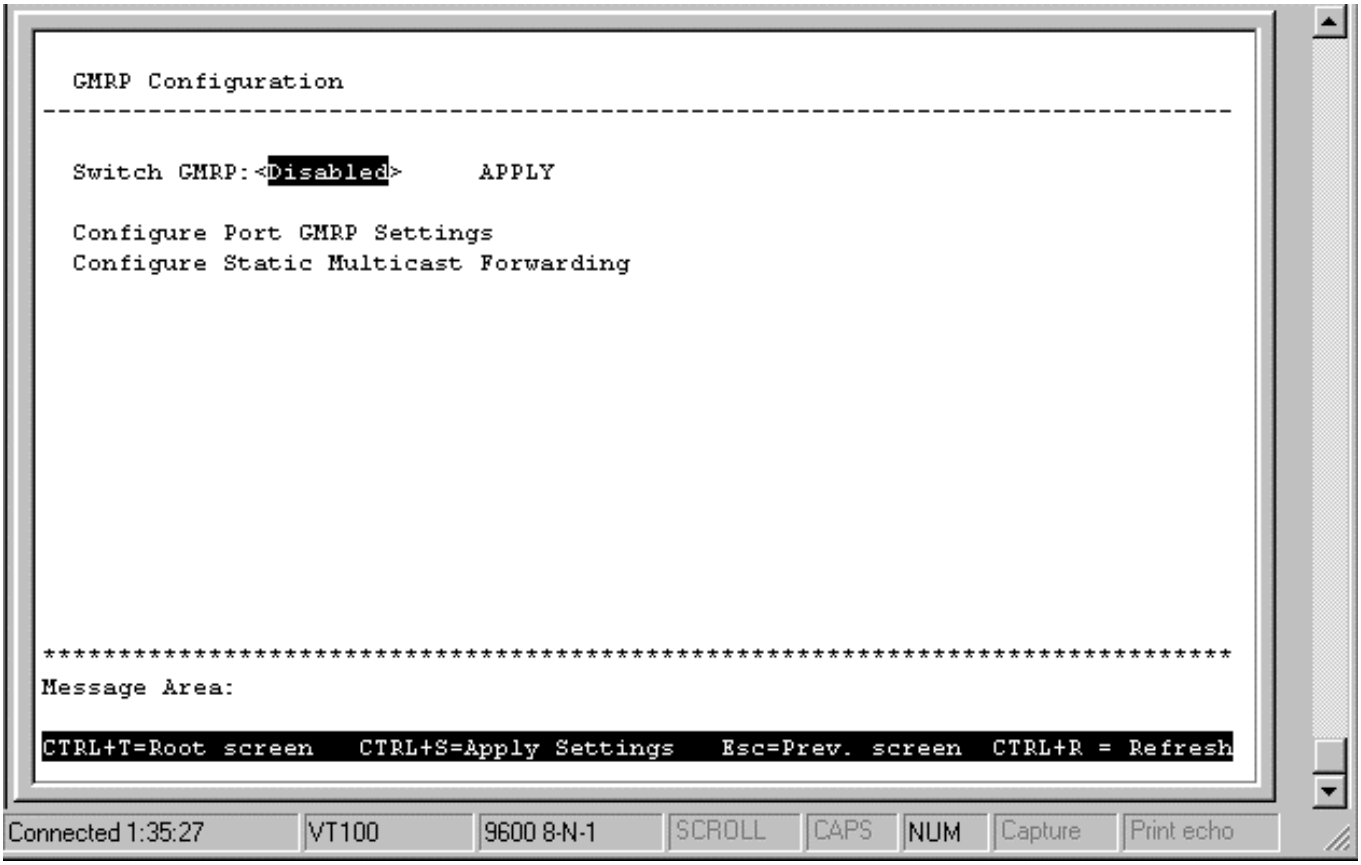


Figure 6-44. the first GMRP Configuration screen

The Switch GMRP field allows you to either enable or disable GMRP on the Switch by toggling between the two choices and then pressing APPLY to let the change take effect.

Once GMRP is enabled for the Switch, you then must enable specific ports by selecting **Configure Port GMRP Settings** from the **GMRP Configuration** screen below. Press APPLY to let your changes take effect.

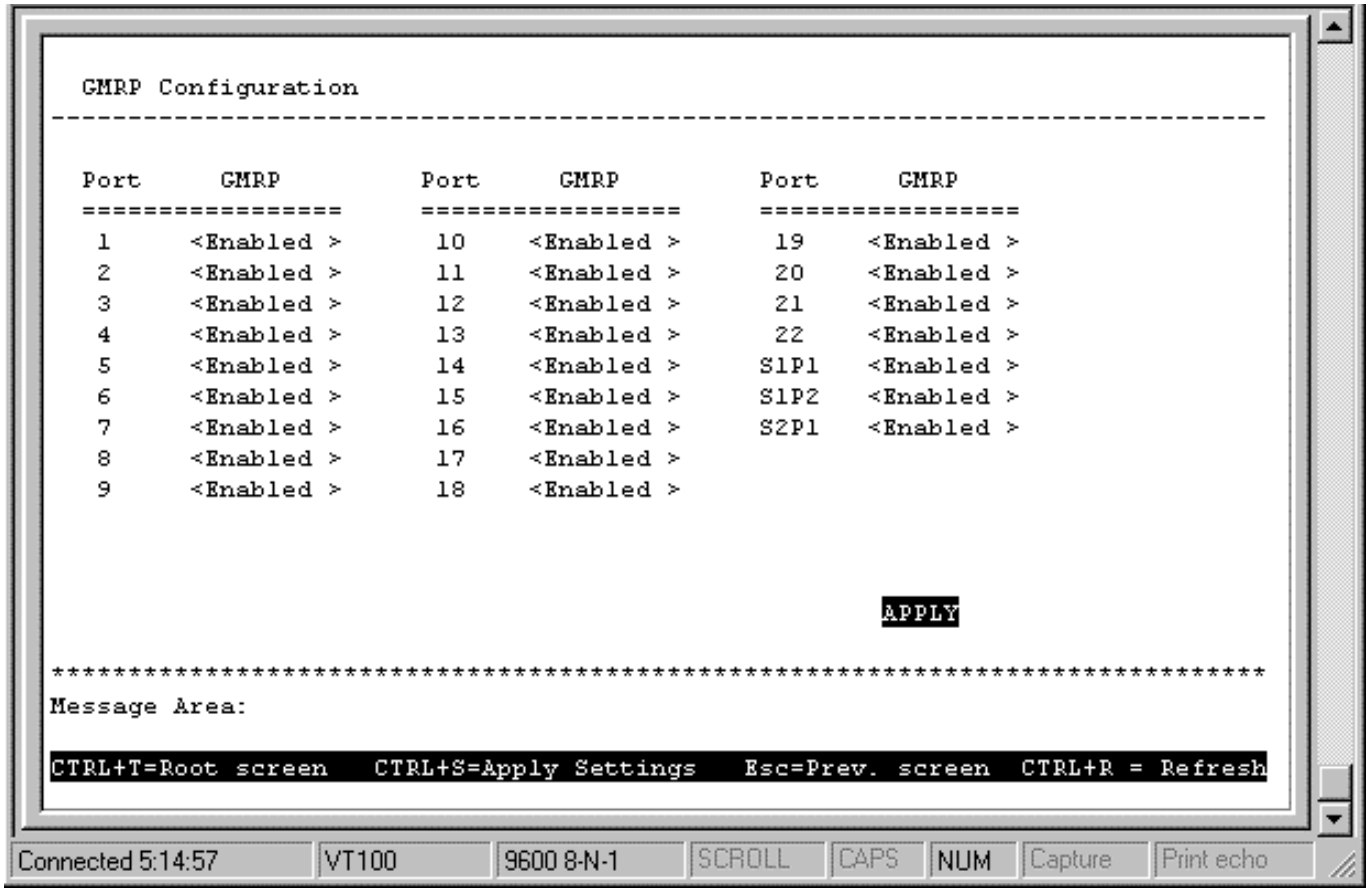


Figure 6-45. the second GMRP Configuration screen

Configure Static Multicast Forwarding

Multicast forwarding allows you to forward traffic over each port for one multicast group.

To access the first version of the **Static Multicast Forwarding Table** (when *IEEE 802.1Q VLANs* is selected on the **VLANs & MAC-based Broadcast Domains Configuration** screen), open **Configuration**, select **Configure VLANs & MAC-based Broadcast Domains**, and then choose **Configure GMRP**. Now select **Configure Static Multicast Forwarding** from the bottom of the **GMRP Configuration** screen. The following screen appears:

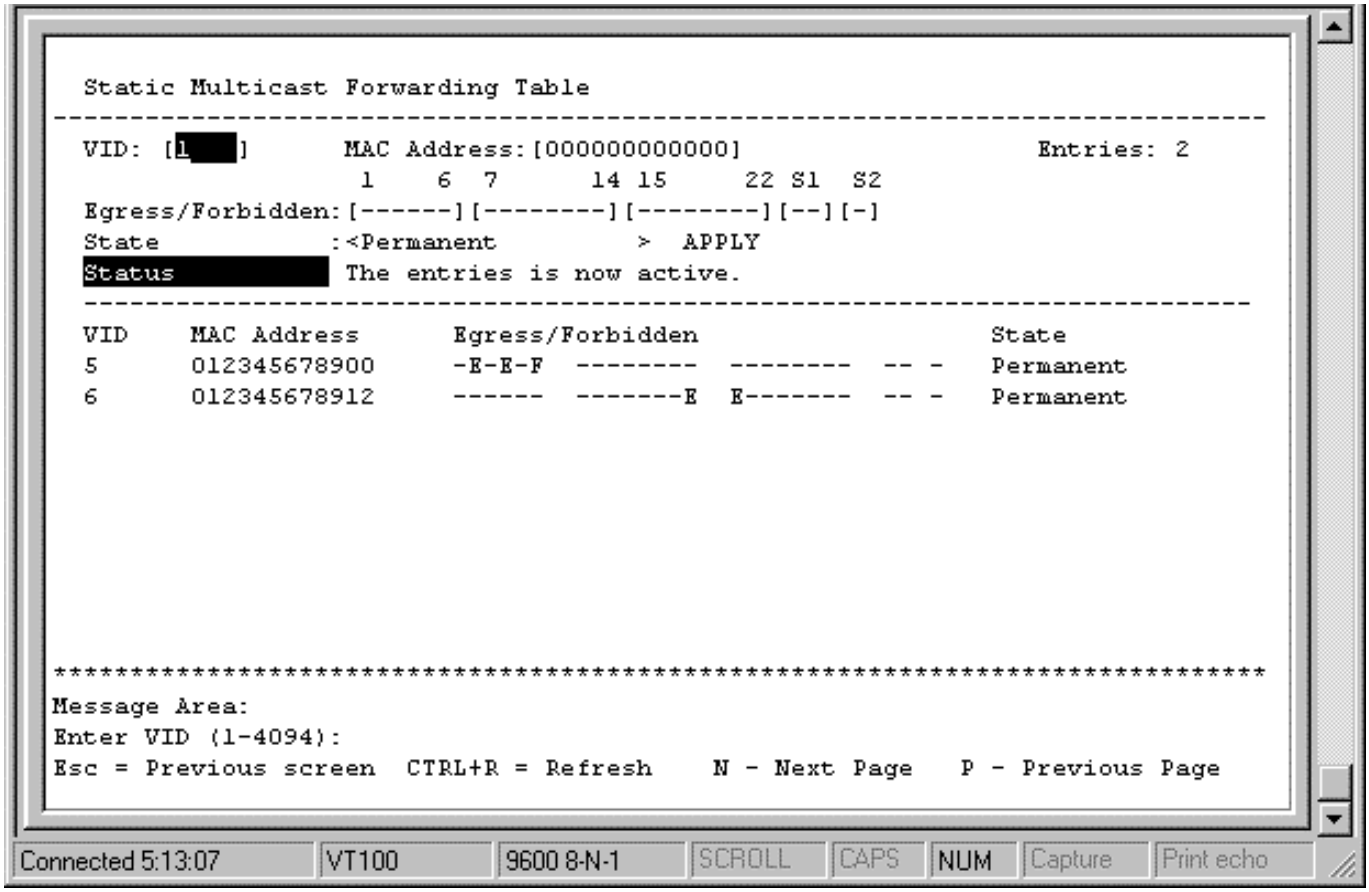


Figure 6-46A. Static Multicast Forwarding Table screen

To add an entry or make a change to an entry on the **Static Multicast Forwarding Table**, enter a VLAN ID, enter a MAC address, choose *Egress* or *Forbidden* for each port, choose a State (*Delete on Reset*, *Delete on Timeout*, *Invalid*, or *Permanent*), and then press APPLY to put the change into effect.

Items in the above window are defined as follows:

- **VID** This is the VLAN that will be defined on this screen. Note a VLAN ID is from 1 to 4094.
- **MAC Address** The MAC address of the newly created Static Multicast Forwarding Table entry.
- **Egress/Forbidden** Position the cursor over the dash "-" representing the appropriate port number and press the <space bar> to select *E* for Egress, *F* for Forbidden, or leave the dash "-". An *E* designates the specified port as a static member of the VLAN. A dash means the port is not given VLAN membership for the VID entered above. An *F* forbids the port from joining a VLAN dynamically.
- **State** Choose how you want the Switch to deal with the newly created Static Multicast Forwarding table entry: *Delete on Reset*, *Delete on Timeout*, *Invalid*, or *Permanent.*

When *Port-Based VLANs*, *MAC-based Broadcast Domains*, or *None* are selected on the **VLANs & MAC-based Broadcast Domains Configuration** screen, the following **Static Multicast Forwarding Table** screen appears:

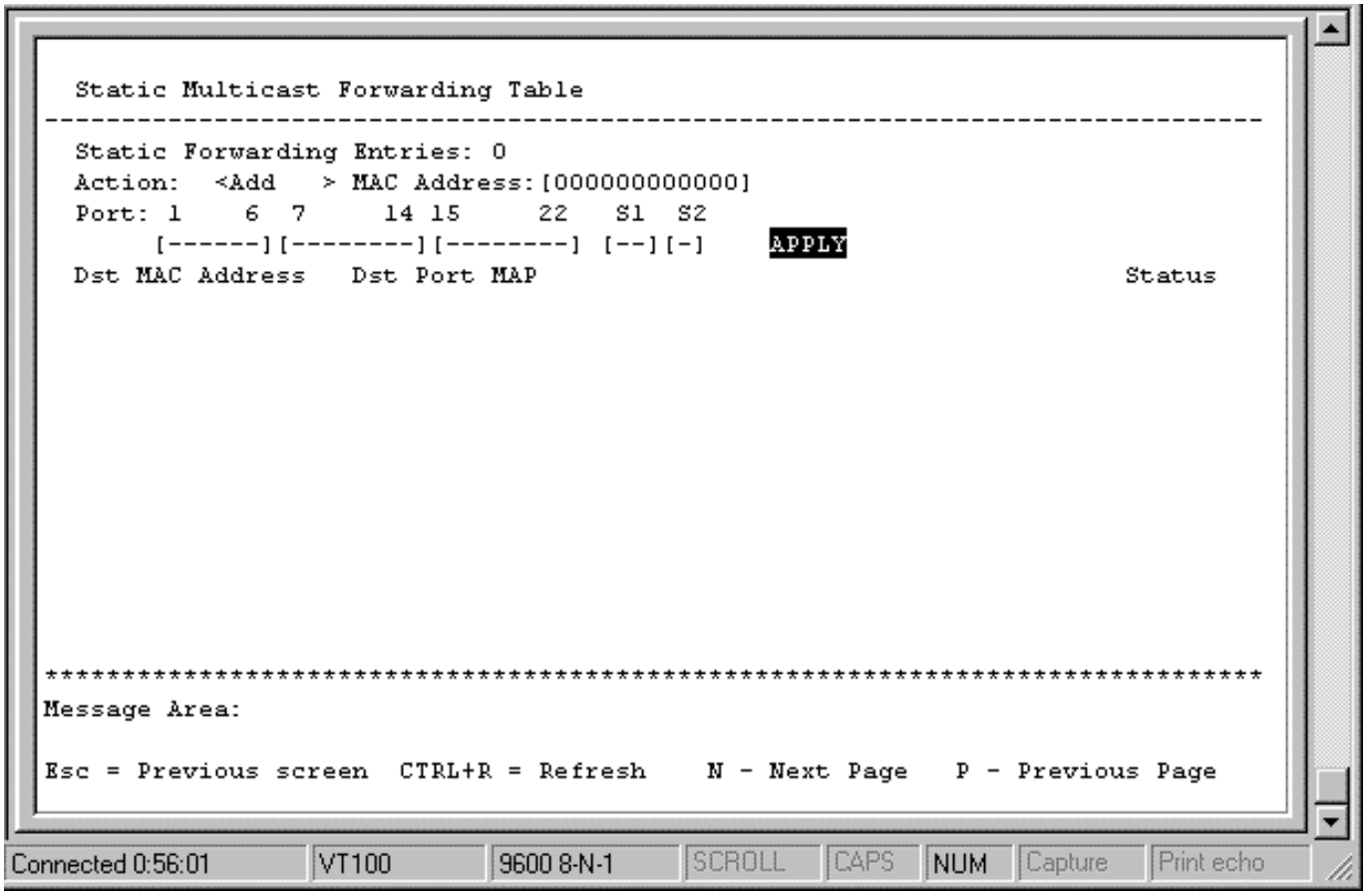


Figure 6-46B. Static Multicast Forwarding Table screen

To add an entry or make a change to an entry on the **Static Multicast Forwarding Table**, select *Add* or *Remove* in the first field, enter the multicast MAC address in the next field, assign the outgoing ports by typing a "V", and then press APPLY to put the changes into effect.

Configure Trunk

Ports on the Switch can be grouped together in a single logical port called a trunk. This is discussed in detail in the *Port Trunking* section of the *Switch Management Concepts* chapter of this manual.

To setup a trunk group, choose **Configure TRUNK** in the **Configuration** menu. The following screen appears:

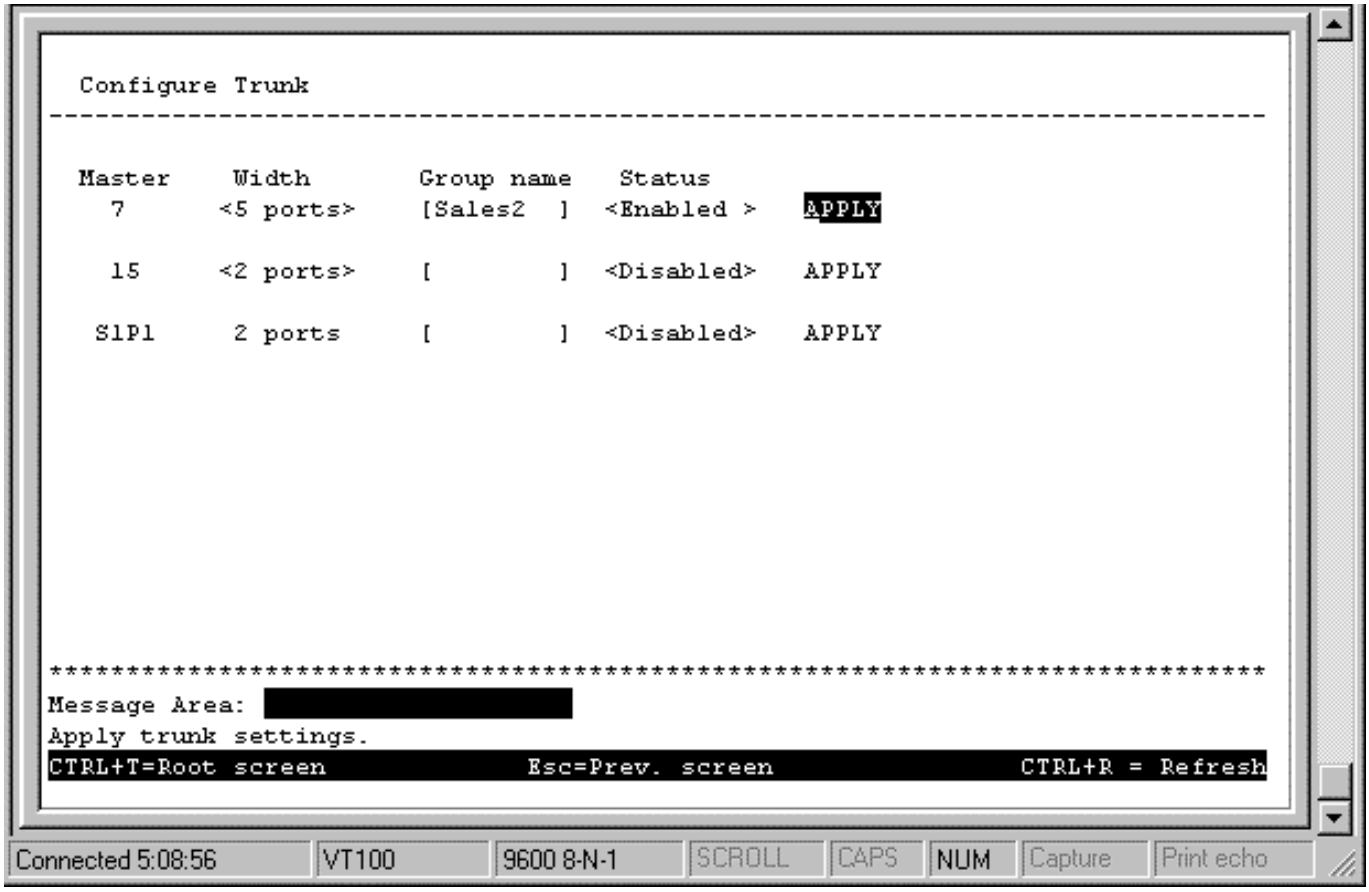


Figure 6-47. Configure Trunk screen

The fields you can set are:

- **Master** There are three listings representing the master port for each of the three trunk groups available on the Switch. The master port for each group is preset and cannot be changed.
- **Width** Select between 2 to 8 ports in the first two entries for this field. The number of ports defined here start from the master port and count up. Thus, in the example pictured above containing a width of 5 ports in the first trunk, the ports in the trunk group will include ports 7 (master), 8, 9, 10 and 11. The third entry (used for 2-port front-panel modules) has a permanent setting of 2 ports.
- **Group name** Enter the desired group name.
- **Status** Enables or disables this trunk group. Be careful when disabling trunk groups as the connections will return to normal operation and may cause signal loops.

Press APPLY to let the changes take effect.

Update Firmware and Configuration Files

The Switch is capable of obtaining its configuration settings (the same settings defined in this console program), as well as updated versions of its internal switching software (the console program itself), using TFTP (Trivial File Transfer Protocol). You can use the **Update Firmware and Configuration Files** screen to control this feature.

Choose **Update Firmware and Configuration Files** to access the fourth item on the Switch's main menu. The following screen appears:

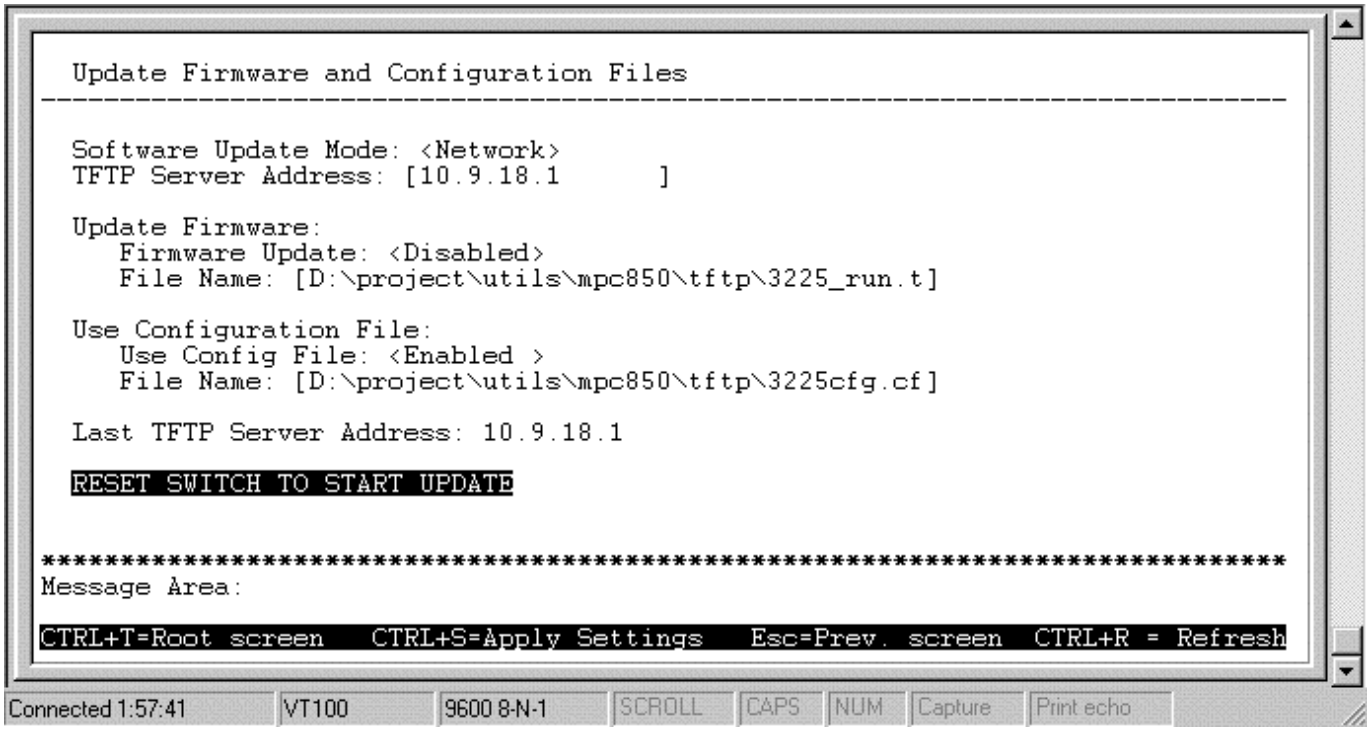


Figure 6-48. Update Firmware and Configuration Files screen

After making your changes in the fields above, press RESET SWITCH TO START UPDATE to initiate the update sequence.

The fields you can set are:

- **TFTP Server Address** The IP address of the TFTP server where the runtime (switching software) or configuration file is located. This entry is used only if the Firmware Update is set to *Enabled*.
- **Firmware Update** Determines whether or not the Switch will try to look for a runtime image file on the TFTP server.
- **File Name** The complete path and filename of the runtime image file on your TFTP server to be uploaded to the switch.
- **Use Config File** Toggle to *Enabled* to use the settings in a configuration text file when the switch is reset (rebooted). The configuration file is explained in detail in the *Sample Configuration File Appendix.*
- **File Name** The complete path and filename on the TFTP server for configuration file to be used.

System Utilities

The **Utilities** menu offers three system utility options, **Ping Test**, **Save Settings to TFTP Server**, and **Save Switch History to TFTP Server**. The following window will be opened:

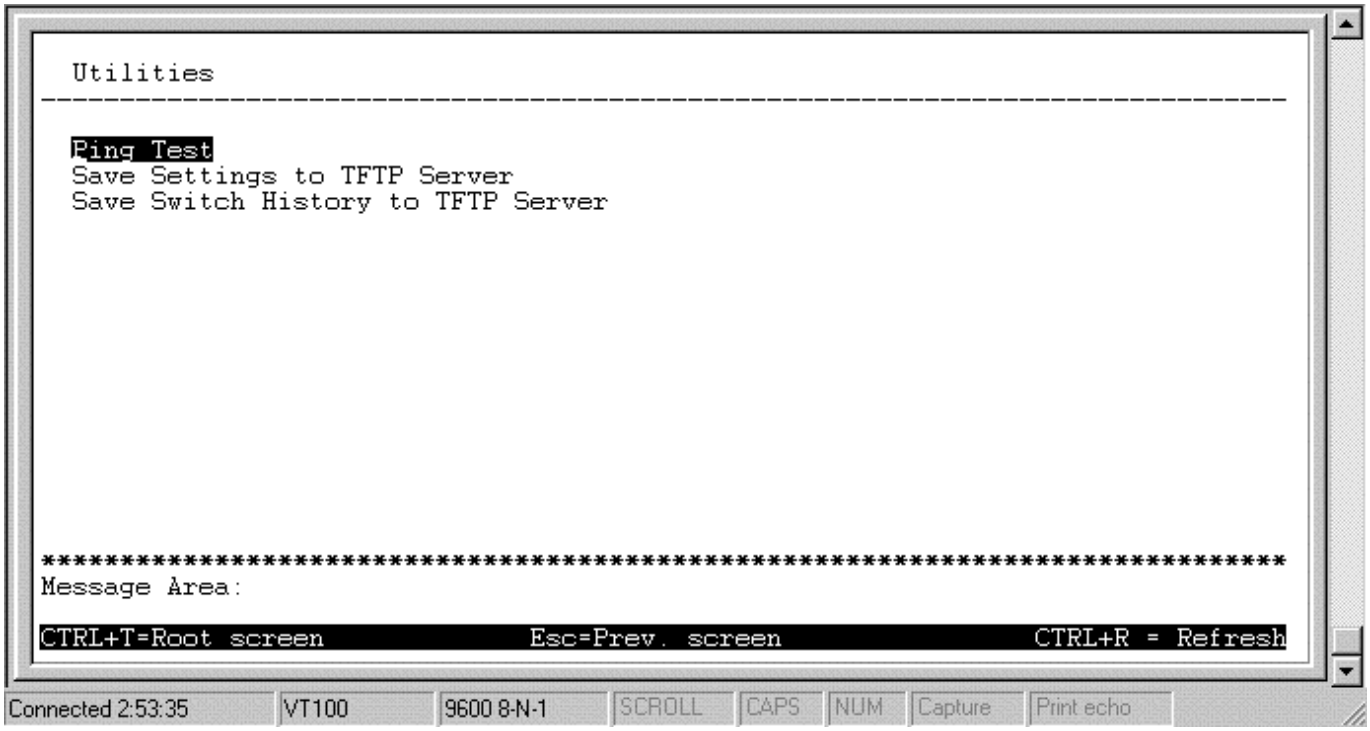


Figure 6-49. Utilities menu

Ping Test

Choose **Ping Test** to access the following screen:

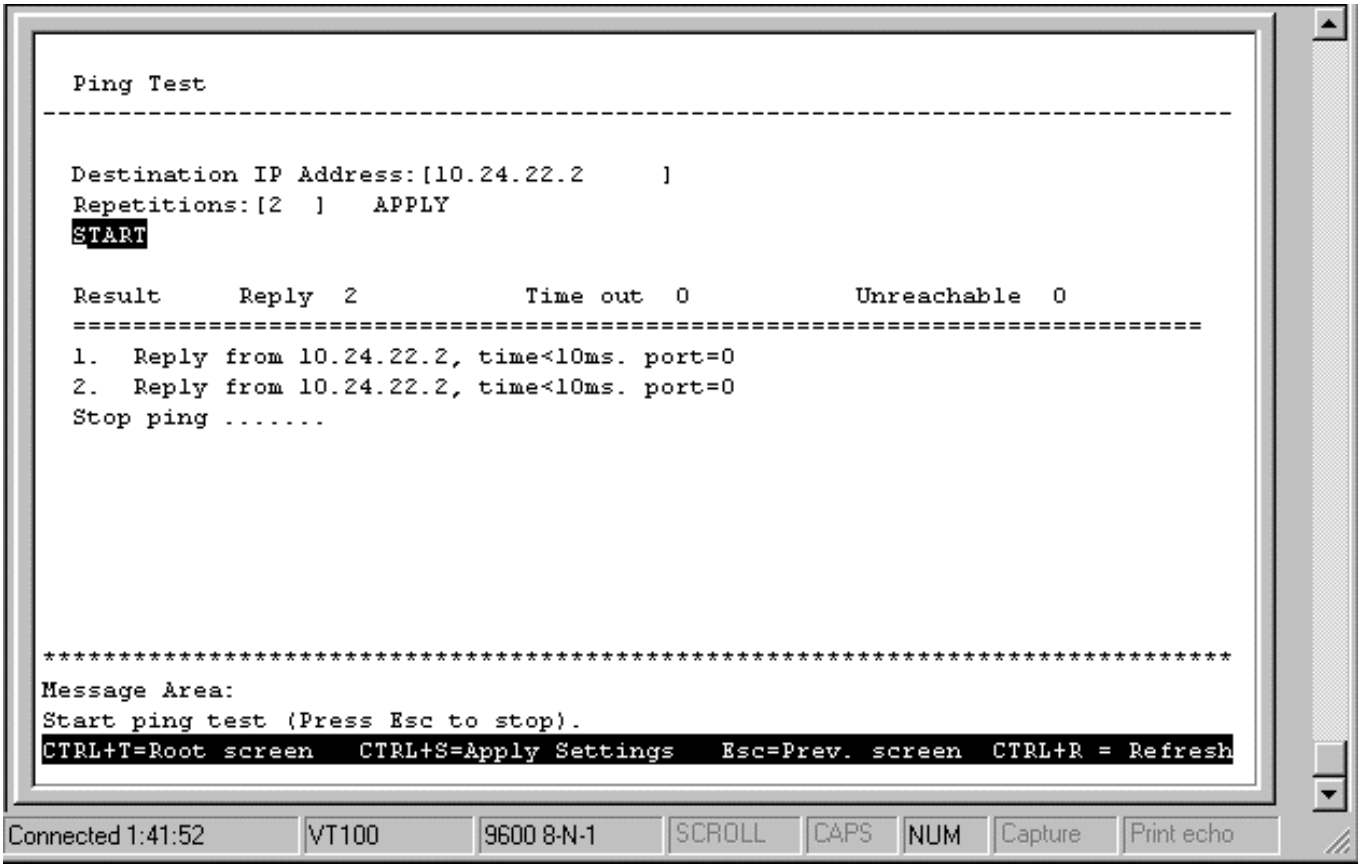


Figure 6-50. Ping Test screen

After filling in the fields above, press START to initiate the Ping test.

The fields you can set are:

- **Destination IP Address** The IP address of the device to be Pinged.
- **Repetitions** Amount of times the Switch should send the Ping (1-255). If zero is chosen, the Switch will continue Pinging indefinitely.

In the lower part of the **Ping Test** screen, you can view the Ping status, including Result, Reply, Time out, and Unreachable.

Save Settings to TFTP Server

Choose **Save Settings to TFTP Server** from the **Utilities** menu (under **System Utilities** on the main menu) to access the following screen:

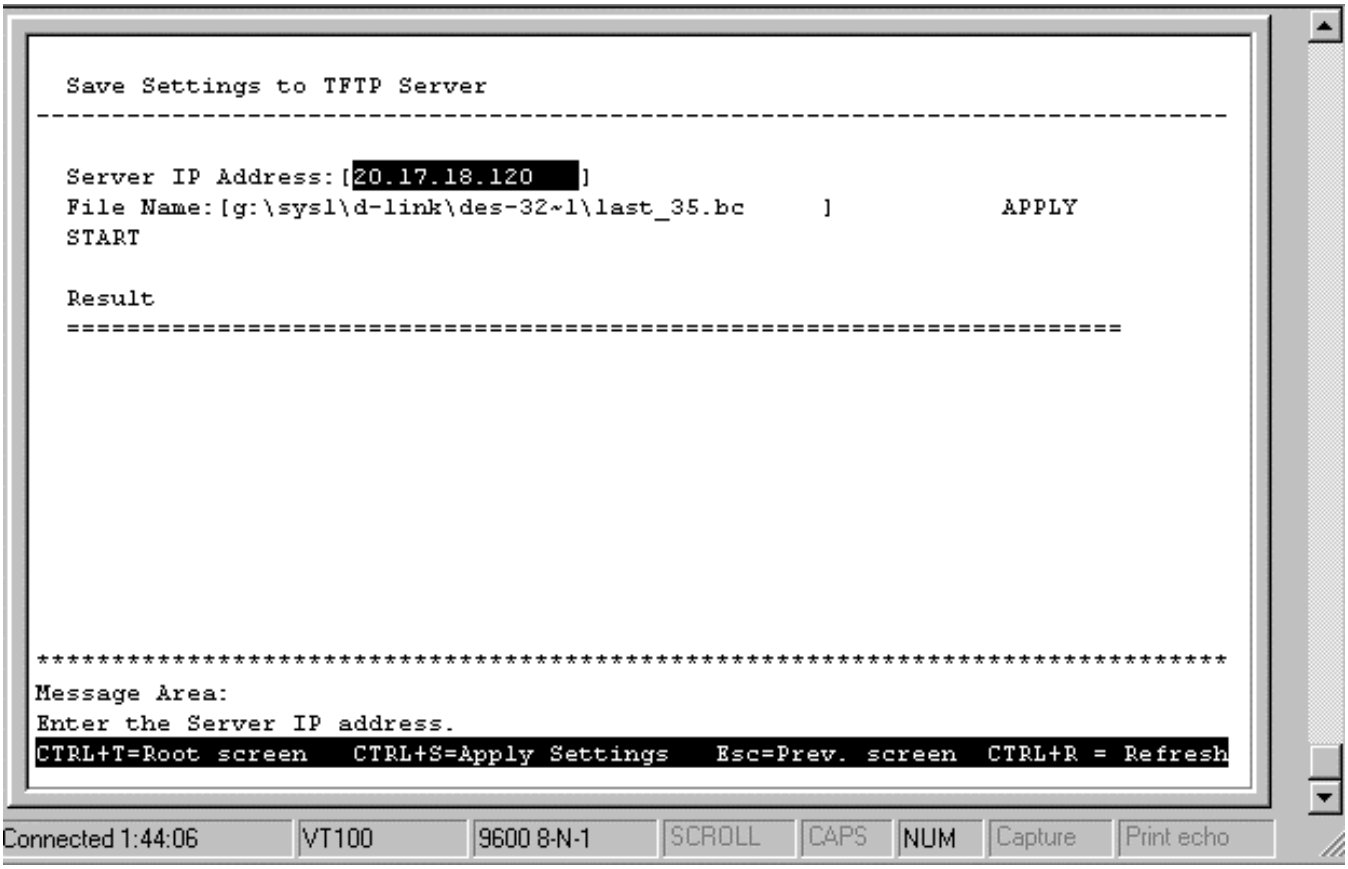


Figure 6-51. Save Settings to TFTP Server screen

The fields you can set are:

- **Server IP Address** The IP address of the TFTP server where you wish to save the settings for the switch.
- **File Name** The complete path and filename for the file.

Press START to begin the saving procedure. The result will be displayed in the lower part of the screen.

Save Switch History to TFTP Server

Choose **Save Switch History to TFTP Server** from the **Utilities** menu (under **System Utilities** on the main menu) to access the following screen:

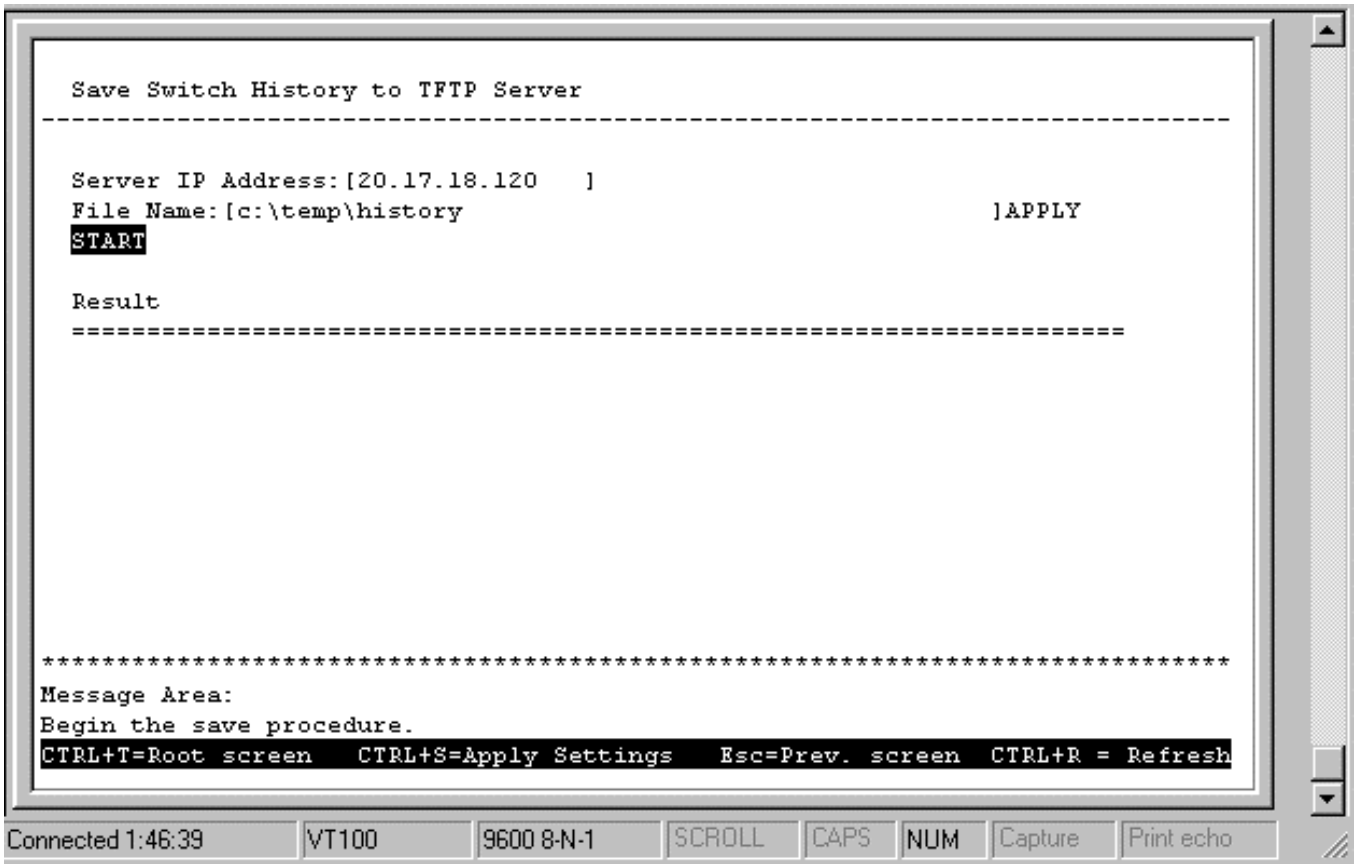


Figure 6-52. Save Switch History to TFTP Server screen

The fields you can set are:

- **Server IP Address** The IP address of the TFTP server where the switch history file will be located.
- **File Name** The complete path and filename on the TFTP server for the file.

Press START to begin the file save. The result will be displayed in the lower part of the screen.

SNMP Manager Configuration

The Switch sends out SNMP *traps* to network management stations whenever certain exceptional events occur, such as when the Switch is turned on or when a system reset occurs. The Switch allows traps to be routed to up to four different network management hosts.

For a detailed list of Trap Types used for this Switch, see the *Traps* section of Chapter 5*, "Switch Management Concepts."*

SNMP (version 1) implements a rudimentary form of security by requiring that each request includes a *community name*. A community name is an arbitrary string of characters used as a "password" to control access to the Switch. If the Switch receives a request with a community name it does not recognize, it will trigger an authentication trap.

The SNMP allows up to four different community names to be defined. The community name **`public`** is defined by default; you can change this name in addition to adding others. You will need to coordinate these names with the community name settings you use in your network management system.

Choose **SNMP Manager Configuration** to access the third item on the main menu. The following screen appears:

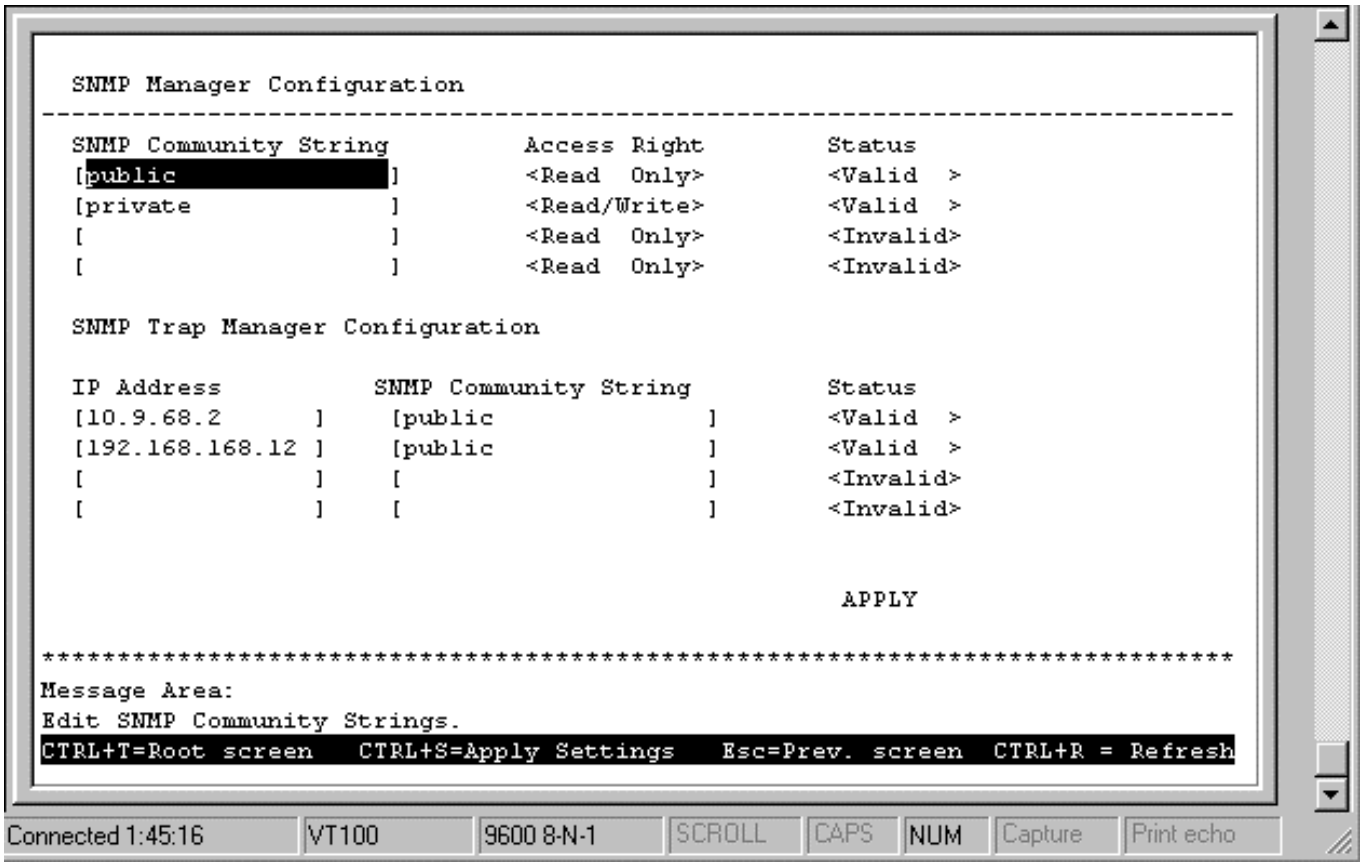


Figure 6-53. SNMP Manager Configuration screen

The following SNMP Manager and Trap Manager Configuration parameters can be set:

- **SNMP Community String** The community string that will be included on SNMP packets sent to and from the switch. Any station not privy to this community will not receive the packet.
- **Access Right** Allows each community to be separately set to either *Read Only,* meaning that the community member can only view switch settings or *Read/Write,* which allows the member to change settings in the switch.
- **Status** Determines whether this community name entry is *Valid* or *Invalid*. An entry can be disabled by changing its status to *Invalid*.
- **IP Address** The IP address of the network management station to receive traps.

Switch Monitoring

The Switch uses an SNMP agent which monitors different aspects of network traffic. The SNMP agent keeps counters and statistics on the operation of the Switch itself, and on each port on the Switch. The statistics obtained can be used to monitor the conditions and general efficiency of the Switch.

Network Monitoring

The **Network Monitoring** menu offers six items, **Traffic Statistics**, **Browse Address Table**, **Browse IGMP Status**, **Browse GVRP Status**, **Browse GMRP Status**, and **Switch History**.

Choose **Network Monitoring** from the main menu. The following menu appears:

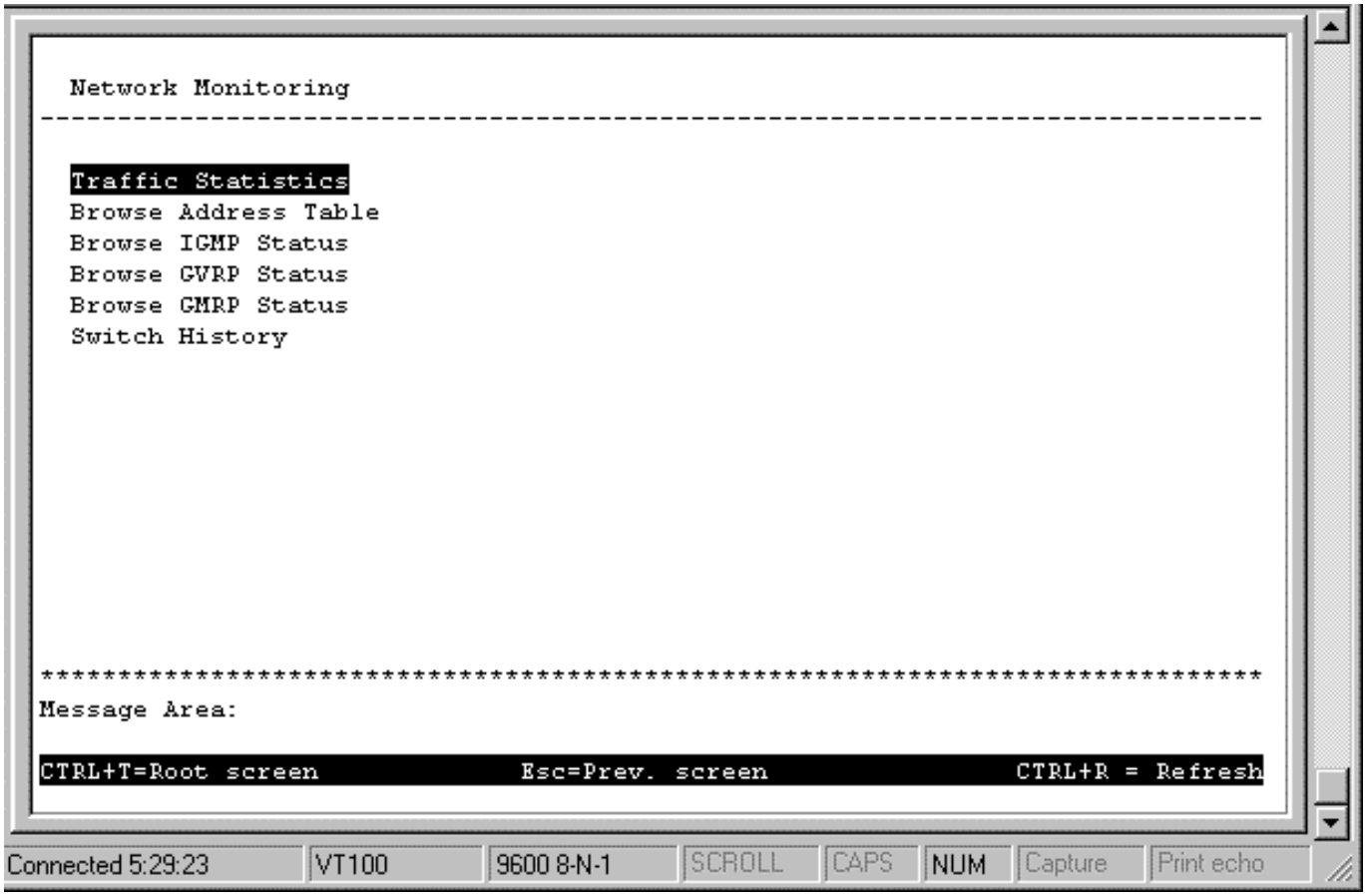


Figure 6-54. Network Monitoring menu

The first item on this menu permits you to access four different tables that observe the condition of each individual port.

Traffic Statistics

To display the **Traffic Statistics** menu, choose the first item on the **Network Monitoring** menu. The following menu appears:

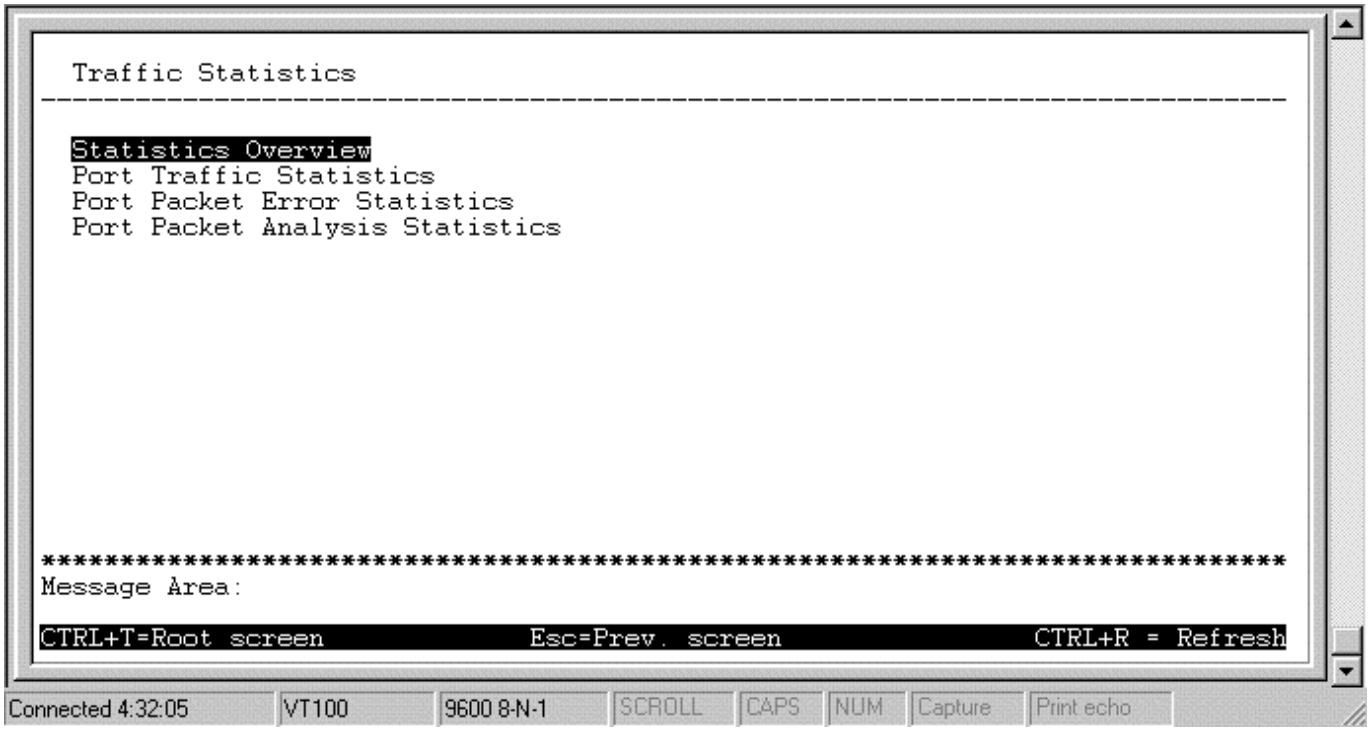


Figure 6-55. Traffic Statistics menu

Statistics Overview

To access the first item on the **Traffic Statistics** menu, choose **Statistics Overview**. The following table appears:

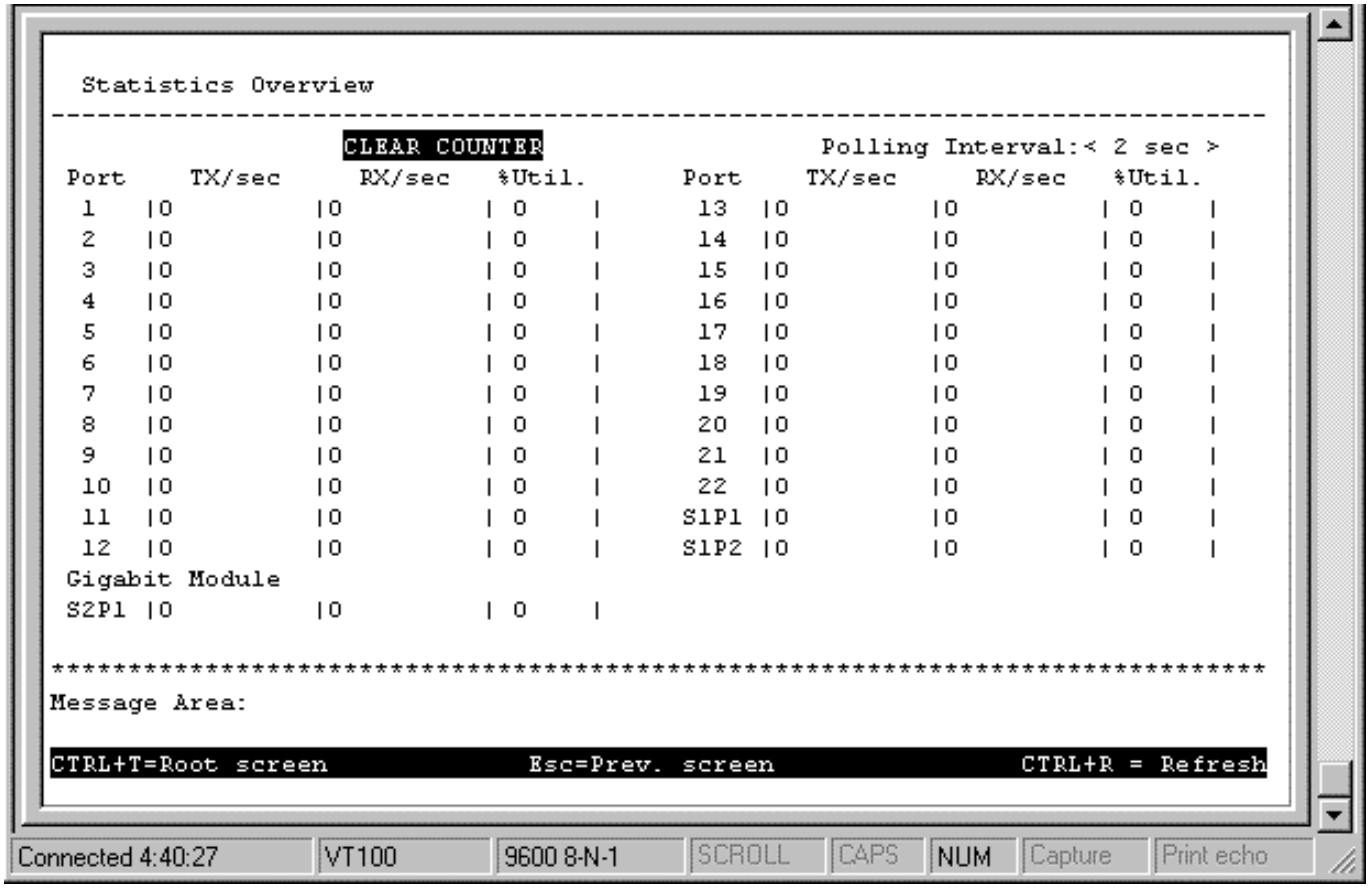

Statistics Overview
CLEAR COUNTER
Polling Interval:< 2 sec >
Port TX/sec RX/sec %Util. Port TX/sec RX/sec %Util.
1 |0 |0 | 0 | 13 |0 |0 | 0 |
2 |0 |0 | 0 | 14 |0 |0 | 0 |
3 |0 |0 | 0 | 15 |0 |0 | 0 |
4 |0 |0 | 0 | 16 |0 |0 | 0 |
5 |0 |0 | 0 | 17 |0 |0 | 0 |
6 |0 |0 | 0 | 18 |0 |0 | 0 |
7 |0 |0 | 0 | 19 |0 |0 | 0 |
8 |0 |0 | 0 | 20 |0 |0 | 0 |
9 |0 |0 | 0 | 21 |0 |0 | 0 |
10 |0 |0 | 0 | 22 |0 |0 | 0 |
11 |0 |0 | 0 | S1P1 |0 |0 | 0 |
12 |0 |0 | 0 | S1P2 |0 |0 | 0 |
Gigabit Module
S2P1 |0 |0 | 0 |
Message Area:
CTRL+T=Root screen Esc=Prev. screen CTRL+R = Refresh
Connected 4:40:27
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 6-56. Statistics Overview screen

Select the desired increment setting in the **Polling Interval** field: *2 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*. Pressing CLEAR COUNTER resets the counters on this screen.

The statistic counters displayed are defined as follows:

- **TX/sec** The number of good bytes sent from the respective port per second.
- **RX/sec** The number of good bytes received per second. This also includes local and dropped packets.
- **%Util.** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval. For example, when a 10 Mbps port is relaying packets at 5 Mbps, the utilization is 50%.

Port Traffic Statistics

To access the second item on the **Traffic Statistics** menu, choose **Port Traffic Statistics**. The following table appears:

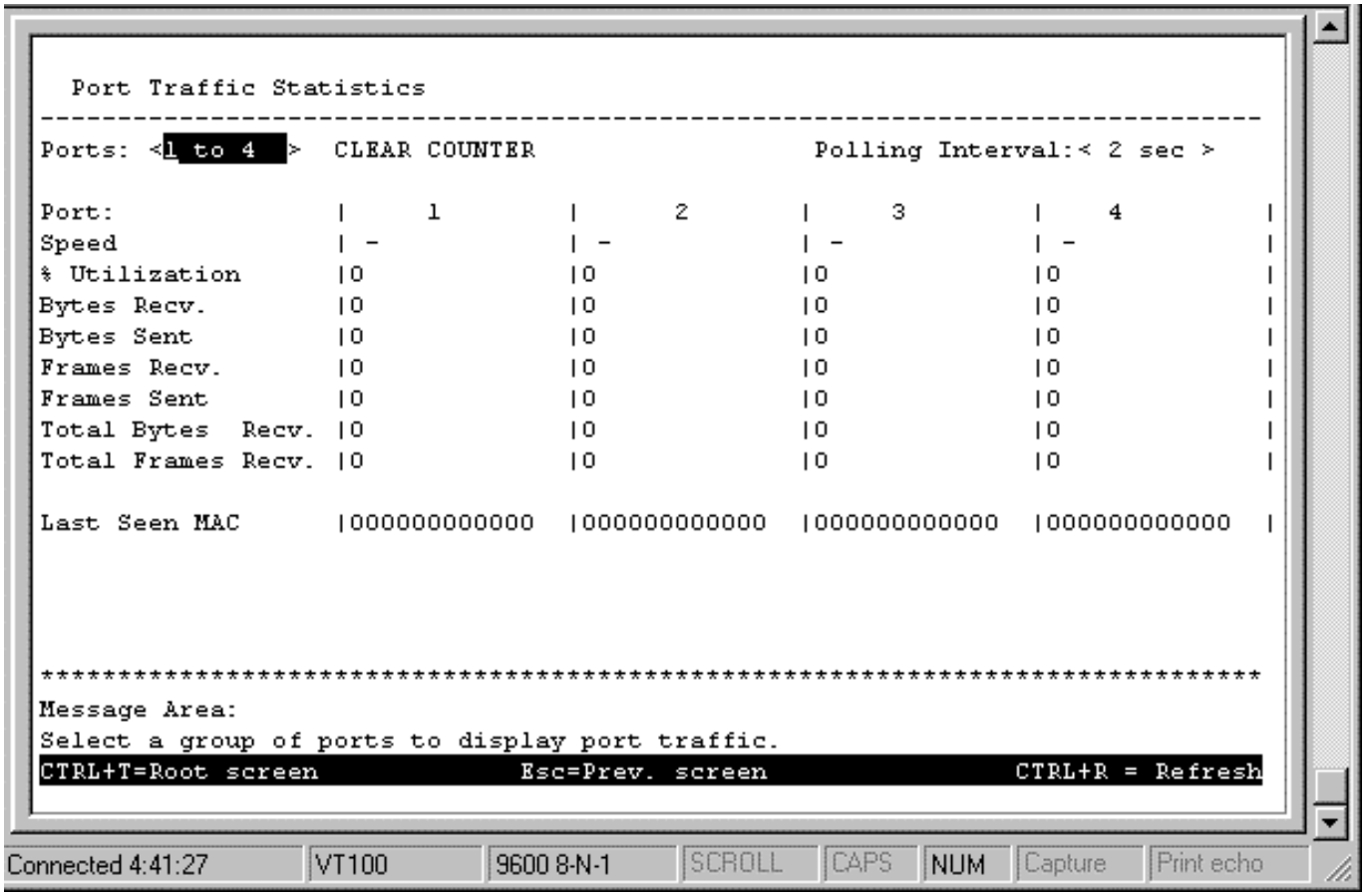

Port Traffic Statistics
Ports: <1 to 4 > CLEAR COUNTER Polling Interval:< 2 sec >
Port: | 1 | 2 | 3 | 4 |
Speed | - | - | - | - |
% Utilization |0 |0 |0 |0 |
Bytes Recv. |0 |0 |0 |0 |
Bytes Sent |0 |0 |0 |0 |
Frames Recv. |0 |0 |0 |0 |
Frames Sent |0 |0 |0 |0 |
Total Bytes Recv. |0 |0 |0 |0 |
Total Frames Recv. |0 |0 |0 |0 |
Last Seen MAC |000000000000 |000000000000 |000000000000 |000000000000 |
Message Area:
Select a group of ports to display port traffic.
CTRL+T=Root screen Esc=Prev. screen CTRL+R = Refresh
Connected 4:41:27
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 6-57. Port Traffic Statistics screen

Select the desired setting in the **Ports** field: *1 to 4*, *5 to 8*, *9 to 12*, *13 to 16*, *17 to 20*, *21-S1P2*, or *Slot 2* and the desired increment setting in the **Polling Interval** field: *2 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*. Pressing CLEAR COUNTER resets the counters on this screen.

The statistic counters displayed are defined as follows:

- **Speed** If the link is up, the speed and duplex status will be displayed; if the link is down "-" will be displayed.
- **% Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval. For example, when a 10 Mbps port is relaying packets at 5 Mbps, the utilization is 50%.
- **Bytes Recv.** The number of good bytes received. This also includes local and dropped packets.
- **Bytes Sent** The number of good bytes sent from the respective port.
- **Frames Recv.** The number of good frames received. This also includes local and dropped packets.
- **Frames Sent** The number of good frames sent from the respective port.
- **Total Bytes Recv.** The number of bytes received, good and bad.
- **Total Frames Recv.** The number of frames received, good and bad.
- **Last Seen MAC** The MAC address of the last device that sent packets over this port.

Port Packet Error Statistics

To access the third item on the **Traffic Statistics** menu, choose **Port Packet Error Statistics**. The following table appears:

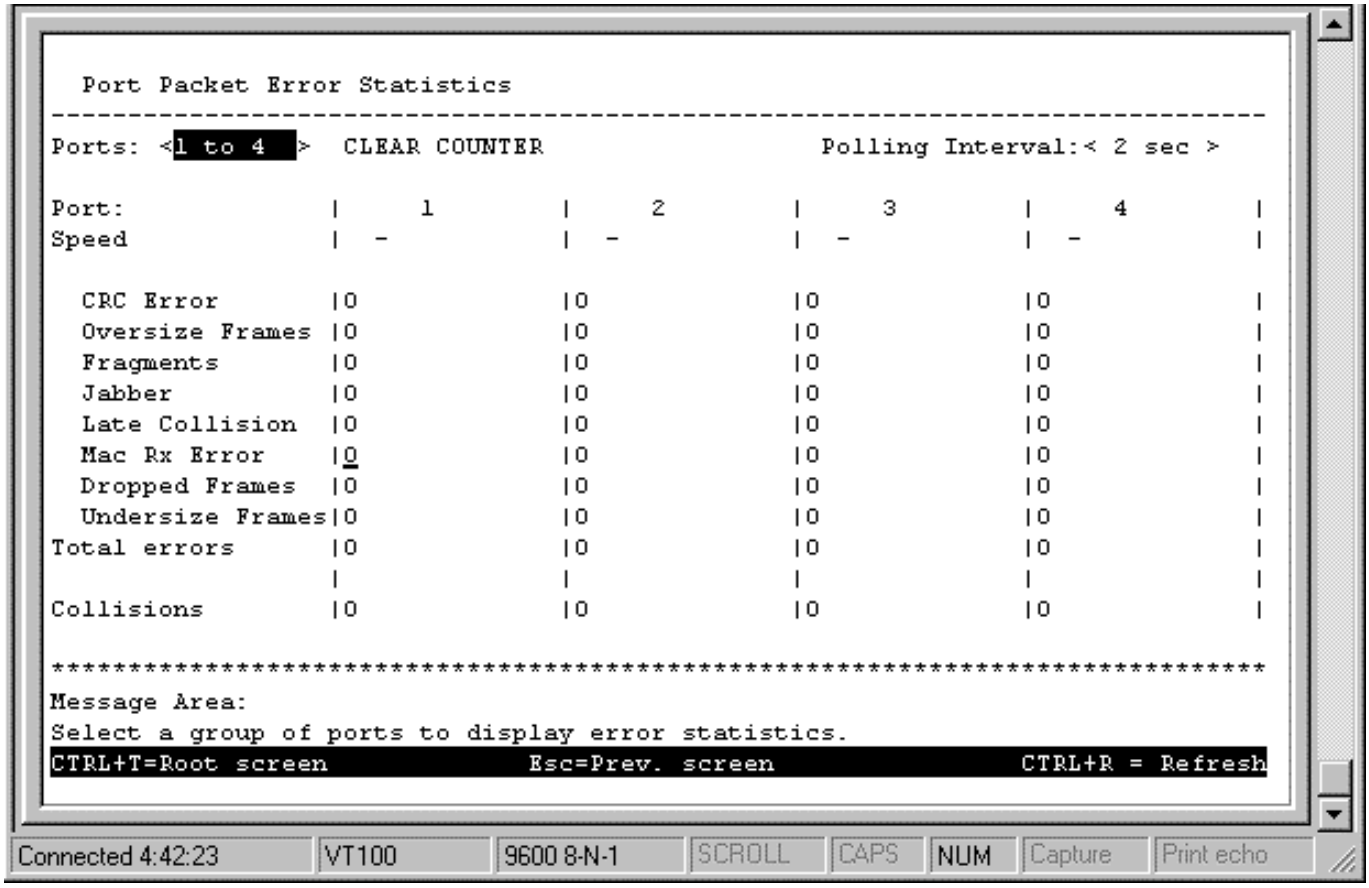

Port Packet Error Statistics
Ports: <1 to 4 > CLEAR COUNTER Polling Interval:< 2 sec >
Port: | 1 | 2 | 3 | 4 |
Speed | - | - | - | - |
CRC Error |0 |0 |0 |0 |
Oversize Frames |0 |0 |0 |0 |
Fragments |0 |0 |0 |0 |
Jabber |0 |0 |0 |0 |
Late Collision |0 |0 |0 |0 |
Mac Rx Error |0 |0 |0 |0 |
Dropped Frames |0 |0 |0 |0 |
Undersize Frames|0 |0 |0 |0 |
Total errors |0 |0 |0 |0 |
Collisions |0 |0 |0 |0 |
Message Area:
Select a group of ports to display error statistics.
CTRL+T=Root screen Esc=Prev. screen CTRL+R = Refresh
Connected 4:42:23
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 6-58. Port Packet Error Statistics table

Select the desired setting in the **Ports** field: *1 to 4*, *5 to 8*, *9 to 12*, *13 to 16*, *17 to 20*, *21-S1P2*, or *Slot 2* and the desired increment setting in the **Polling Interval** field: *2 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*. Pressing CLEAR COUNTER resets the counters on this screen.

The statistic counters displayed are defined as follows:

- **Speed** If the link is up, the speed and duplex status will be displayed; if the link is down "-" will be displayed.
- **CRC Error** The number of frames that fail the CRC integrity check.
- **Oversize Frames** The number of good frames with length greater than 1518 bytes and therefore are greater than the maximum legal length.
- **Fragments** The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
- **Jabber** The number of frames with length more than 1518 bytes and with CRC error or misalignment (bad framing).
- **Late Collision** The number of collisions that occur at or after the 64th byte (octet) in the frame.
- **Mac Rx Error** The number of frames with received MAC Errors.

- **Dropped Frames** The number of frames which are dropped by this port since the last Switch reboot.
- **Undersize Frames** The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
- **Total errors** The sum of the CRC Error, Oversize Frames, Fragments, Jabber, Late Collision, Mac Rx Error, Dropped Frames, and Undersize Frames counters.
- **Collisions** The number of collision that has occurred.

Port Packet Analysis Statistics

To access the fourth item on the **Traffic Statistics** menu, choose **Port Packet Analysis Statistics**. The following table appears:

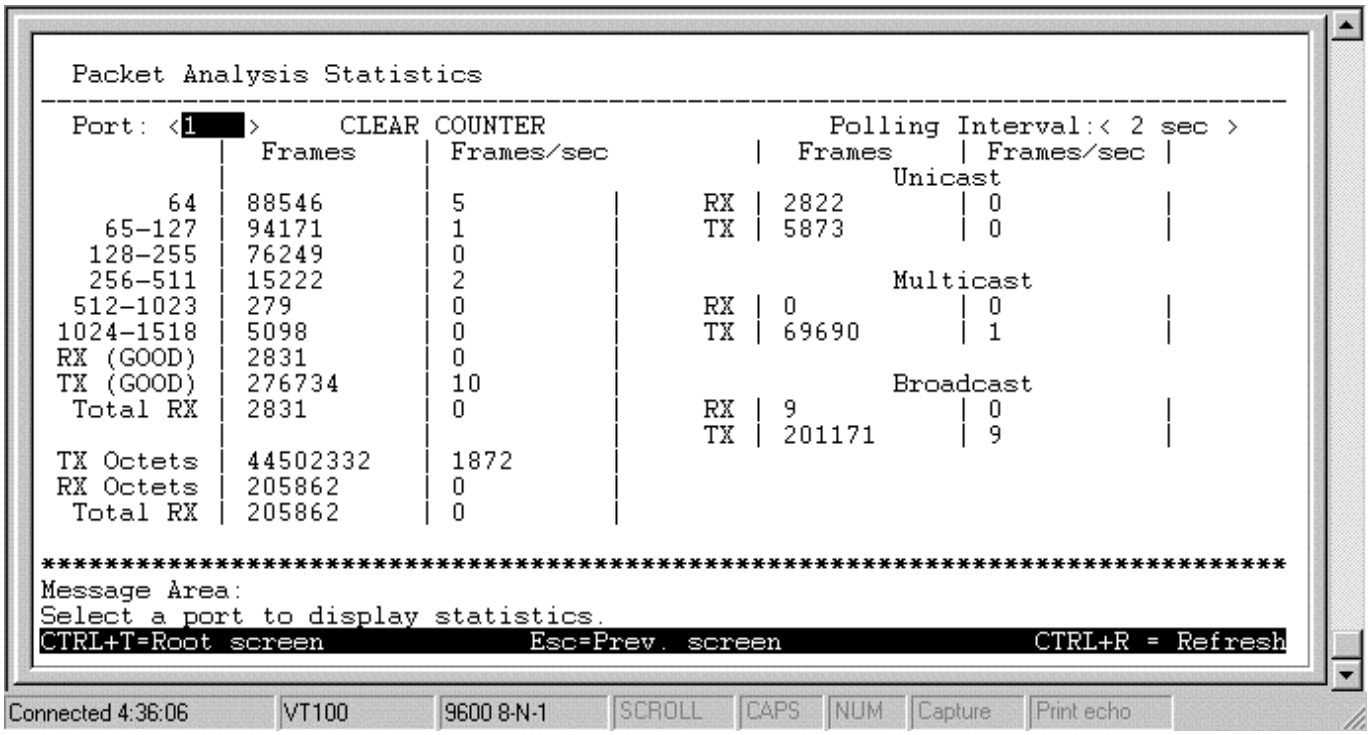

Packet Analysis Statistics
Port: <1> CLEAR COUNTER Polling Interval:< 2 sec >
Frames | Frames/sec | Frames | Frames/sec
Unicast
64 | 88546 | 5 | RX | 2822 | 0
65-127 | 94171 | 1 | TX | 5873 | 0
128-255 | 76249 | 0
256-511 | 15222 | 2
Multicast
512-1023 | 279 | 0 | RX | 0 | 0
1024-1518 | 5098 | 0 | TX | 69690 | 1
RX (GOOD) | 2831 | 0
TX (GOOD) | 276734 | 10
Broadcast
Total RX | 2831 | 0 | RX | 9 | 0
TX | 201171 | 9
TX Octets | 44502332 | 1872
RX Octets | 205862 | 0
Total RX | 205862 | 0
Message Area:
Select a port to display statistics.
CTRL+T=Root screen Esc=Prev. screen CTRL+R = Refresh
Connected 4:36:06 VT100 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure 6-59. Packet Analysis Statistics table

Select the desired setting in the **Ports** field: *1 to 4*, *5 to 8*, *9 to 12*, *13 to 16*, *17 to 20*, *21-S1P2*, or *Slot 2* and the desired increment setting in the **Polling Interval** field: *2 sec*, *5 sec*, *15 sec*, *30 sec*, *1 min*, or *Suspend*. Pressing CLEAR COUNTER resets the counters.

The statistic counters displayed are defined as follows:

- **64**, **65-127**, **128-255**, **256-511**, **512-1023**, **1024-1518** The number of good frames of various length ranges, both valid and invalid.
- **RX (GOOD)** The number of good frames received. This also includes local and dropped packets.
- **TX (GOOD)** The number of good frames sent from the respective port.
- **Total RX** The number of frames received, good and bad.
- **TX Octets** The number of good bytes sent from the respective port.

- **RX Octets** The number of good bytes received. This also includes local and dropped packets.
- **Total RX** The number of bytes received, good and bad.
- **Unicast RX/Unicast TX** The number of good unicast frames received and sent. This includes dropped unicast packets.
- **Multicast RX/Multicast TX** The number of good multicast frames received and sent. This includes local and dropped multicast packets.
- **Broadcast RX/Broadcast TX** The number of good broadcast frames received and sent. This includes dropped broadcast packets.

Browse Address Table

The **Browse Address Table** allows the user to view which Switch port(s) a specific network device uses to communicate on the network. You can sort this table by MAC address, port, or VLAN. This is useful for viewing which ports one device is using, or which devices are using one port.

To display the **Browse Address Table**, choose **Network Monitoring** from the main menu and then choose **Browse Address Table**. The following screen appears:

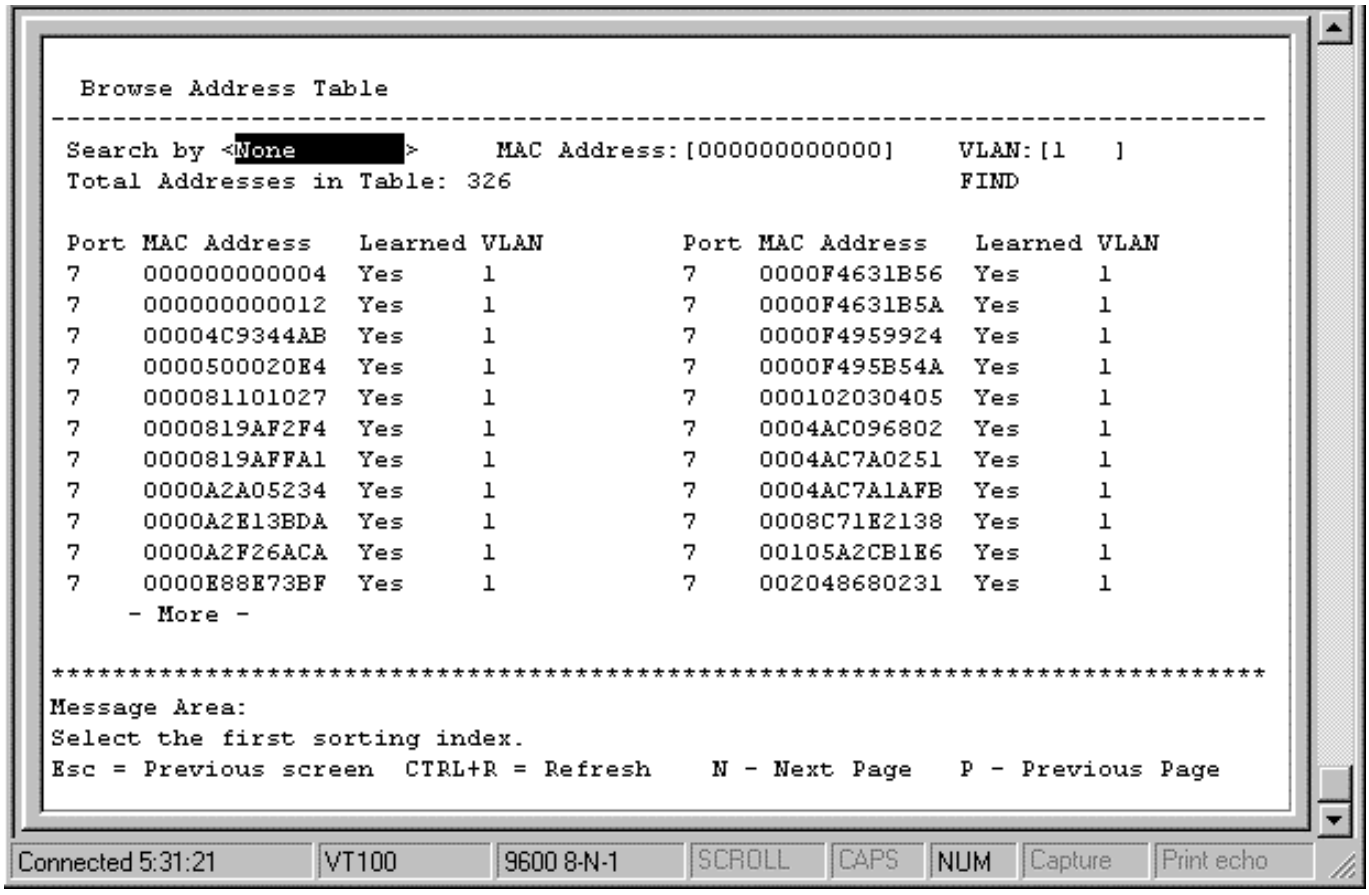

Browse Address Table
Search by <None> MAC Address:[000000000000] VLAN:[1]
Total Addresses in Table: 326 FIND
Port MAC Address Learned VLAN Port MAC Address Learned VLAN
7 000000000004 Yes 1 7 0000F4631B56 Yes 1
7 000000000012 Yes 1 7 0000F4631B5A Yes 1
7 00004C9344AB Yes 1 7 0000F4959924 Yes 1
7 0000500020E4 Yes 1 7 0000F495B54A Yes 1
7 000081101027 Yes 1 7 000102030405 Yes 1
7 0000819AF2F4 Yes 1 7 0004AC096802 Yes 1
7 0000819AFFA1 Yes 1 7 0004AC7A0251 Yes 1
7 0000A2A05234 Yes 1 7 0004AC7A1AFB Yes 1
7 0000A2E13BDA Yes 1 7 0008C71E2138 Yes 1
7 0000A2F26ACA Yes 1 7 00105A2CB1E6 Yes 1
7 0000E88E73BF Yes 1 7 002048680231 Yes 1
- More -
Message Area:
Select the first sorting index.
Esc = Previous screen CTRL+R = Refresh N - Next Page P - Previous Page
Connected 5:31:21
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 6-60. Browse Address Table

To browse by MAC address, select *MAC address* in the Search by field, enter the desired MAC address in the next field, and then press FIND.

To browse by port number, select *Port* in the Search by field, enter the desired port in the next field, and then press FIND.

To browse by VLAN, select VLAN in the Search By field, enter the desired VLAN in the next field, and then press FIND.

The lower part of the screen is a read-only Browse Address Table that contains **Port**, **MAC Address**, **Learned** status, and the **VLAN** number of each entry. Use N to advance to the next page and P to return to the previous page.

Browse IGMP Status

The **Browse IGMP Status** function allows you to browse Internet Group Management Protocol (IGMP). The Switch is able to recognize IGMP queries and reports sent between stations and an IGMP router. When enabled for IGMP snooping, the Switch can open or close a port to specific devices based on the IGMP messages sent from the device to the router or vice versa.

To display the **IP Multicast Information** screen, choose **Network Monitoring** from the main menu and then choose **Browse IGMP Status**. The following screen appears:

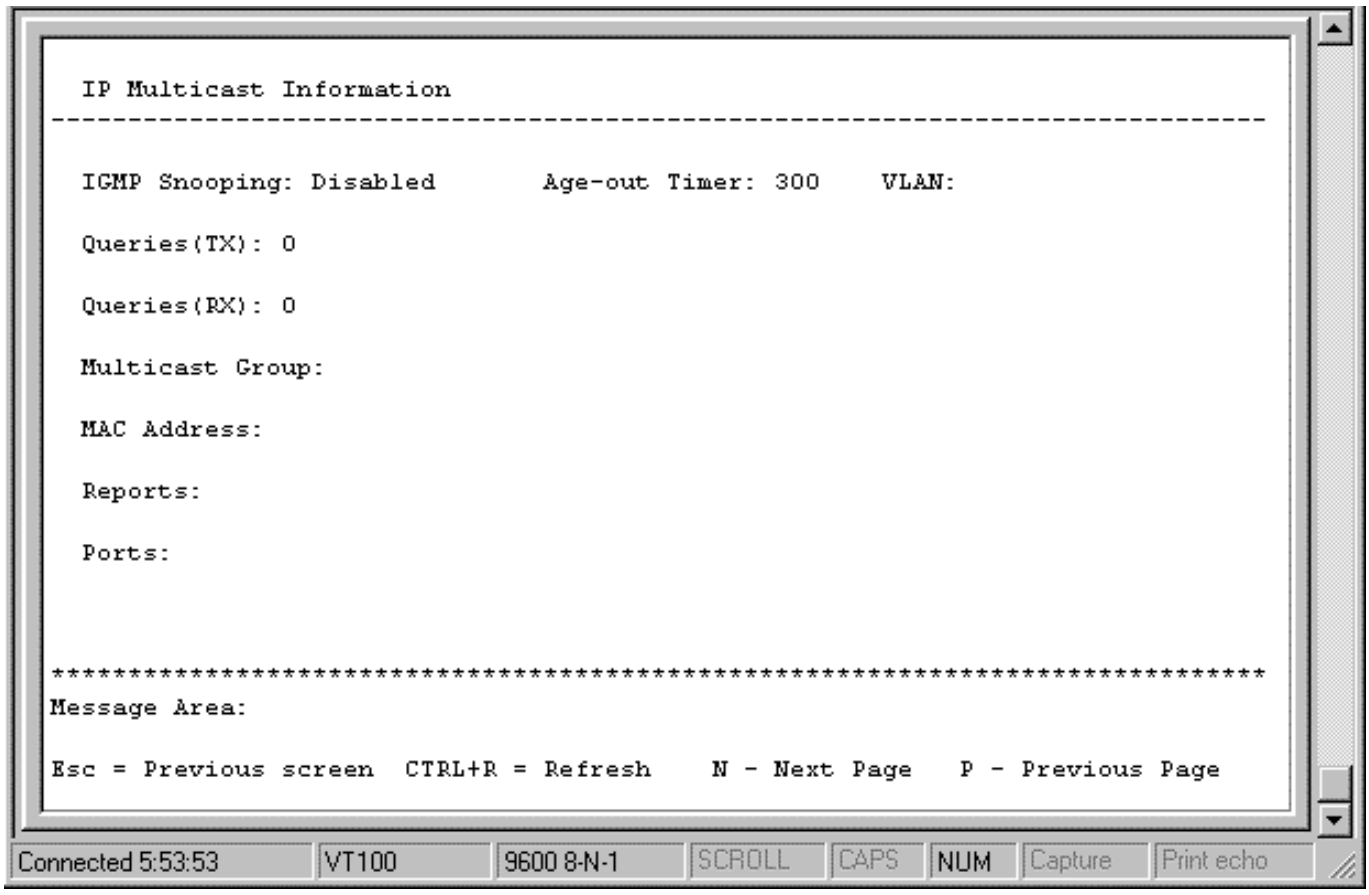


Figure 6-61. IP Multicast Information screen

This screen displays the number of IGMP queries and reports for each active IP multicast group detected by the Switch. You can also view which Switch ports support each multicast group.

The fields displayed are defined as follows:

- **IGMP Snooping** Indicates whether IGMP snooping is *Enabled* or *Disabled*.
- **Age-out Timer** Displays the time the Switch waits between IGMP queries.
- **VLAN** The selected VLAN.

- **Multicast Group** The Multicast IP address of the Multicast group being displayed.
- **MAC Address** The Multicast MAC address of the multicast group being displayed.
- **Queries(TX)** The number of IGMP requests sent by the Switch.
- **Queries(RX)** The number of IGMP requests that have arrived at a Switch port.
- **Reports** The number of notifications sent from each station to the IGMP host, signifying that the station is still (or wants to be) part of a multicast group.
- **Ports** The Switch ports supporting the selected multicast group.

Browse GVRP Status

The **Browse GVRP Status** function allows you to browse GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP).

To display the **GVRP Status** screen, choose **Network Monitoring** from the main menu and then choose **Browse GVRP Status**. The following screen appears:

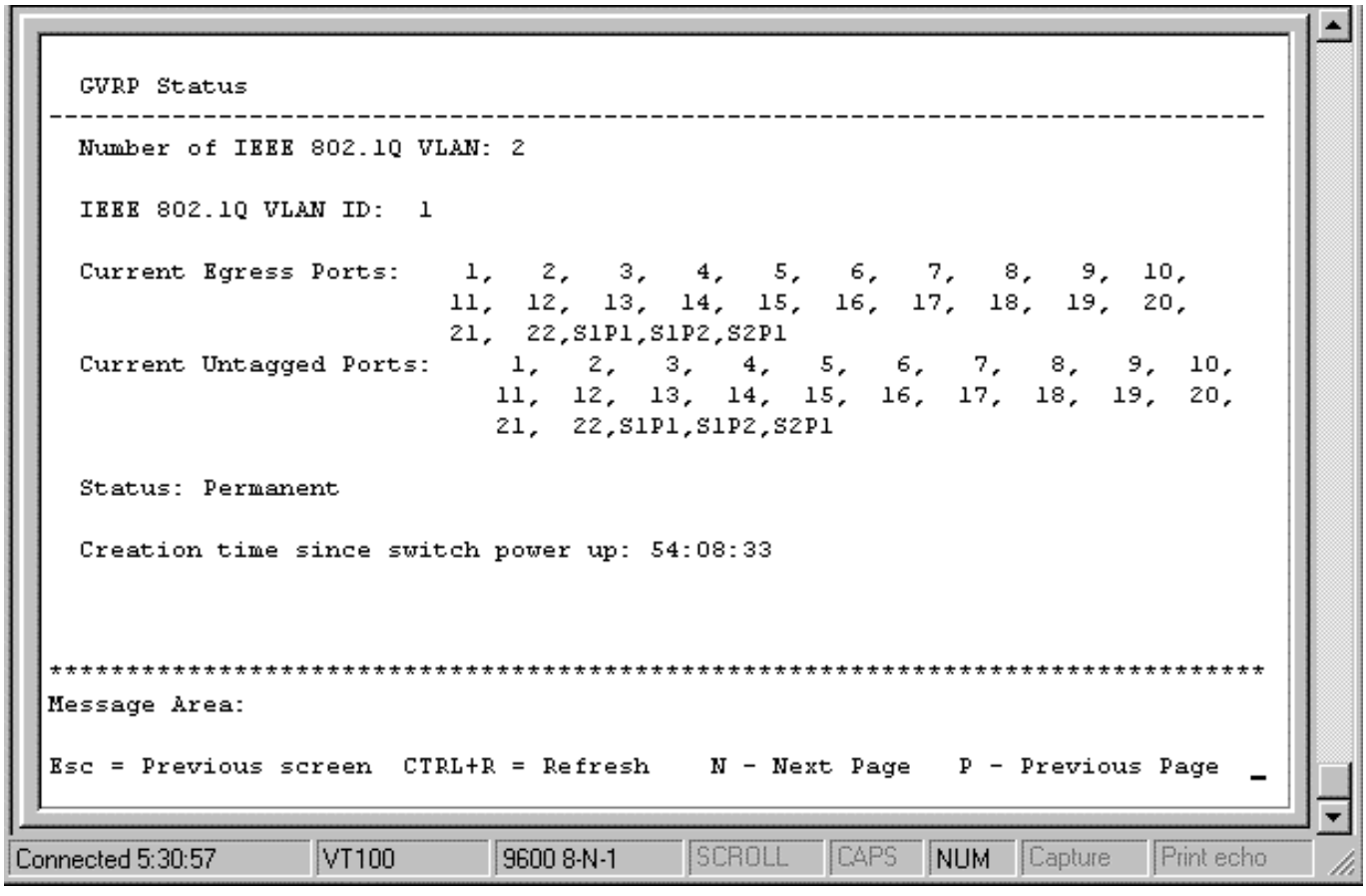

GVRP Status
Number of IEEE 802.1Q VLAN: 2
IEEE 802.1Q VLAN ID: 1
Current Egress Ports: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22,S1P1,S1P2,S2P1
Current Untagged Ports: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22,S1P1,S1P2,S2P1
Status: Permanent
Creation time since switch power up: 54:08:33
Message Area:
Esc = Previous screen CTRL+R = Refresh N - Next Page P - Previous Page
Connected 5:30:57
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 6-62. GVRP Status screen

This screen contains information pertaining to GVRP status.

Browse GMRP Status

The **Browse GMRP Status** function allows you to browse Group Multicast Registration Protocol (GMRP).

To display the **GMRP Status** screen, choose **Network Monitoring** from the main menu and then choose **Browse GMRP Status**. The following screen appears:

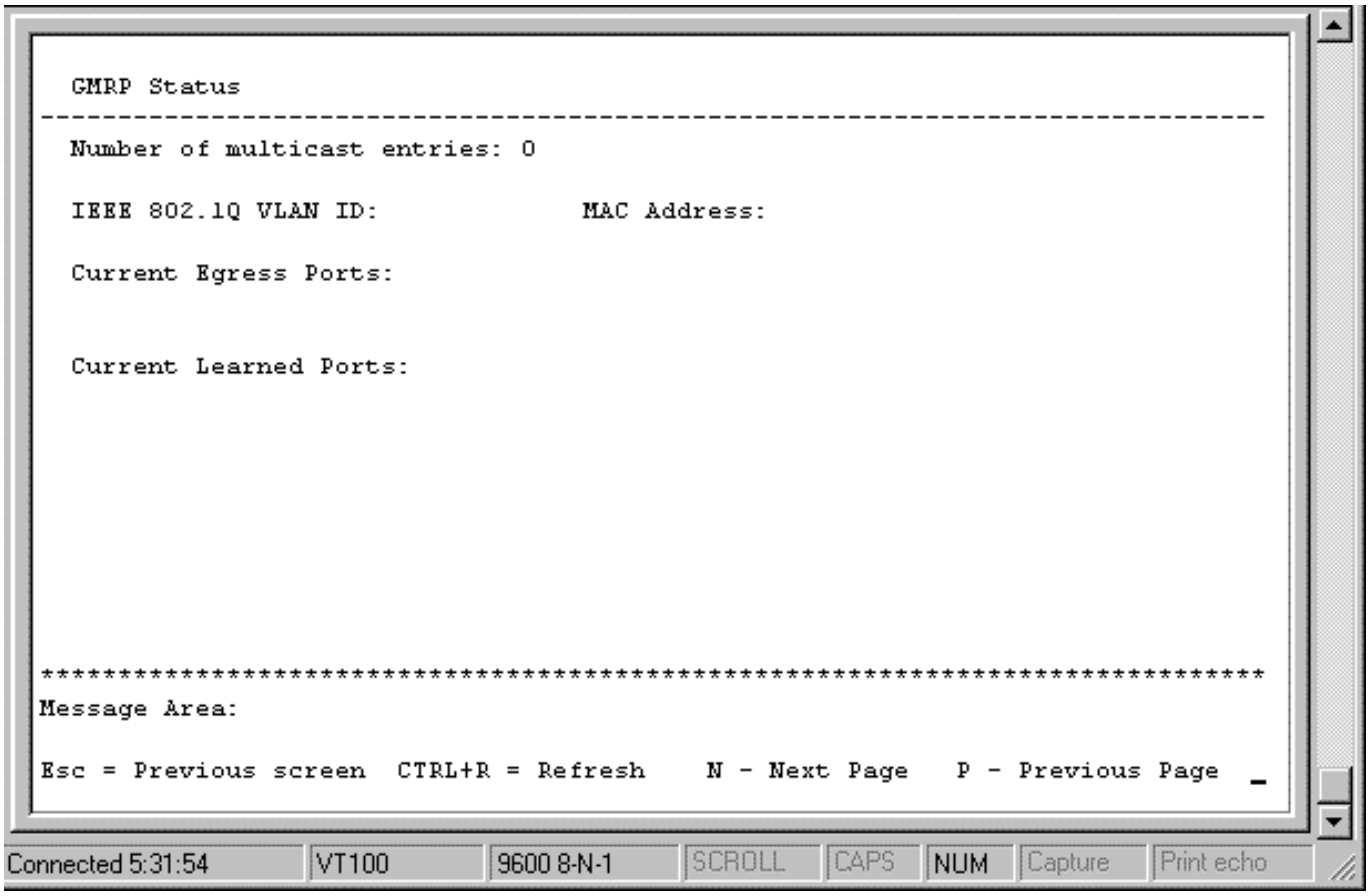


Figure 6-63. GMRP Status screen

This screen displays various pieces of information relating to GMRP status.

Switch History

The **Network Monitoring** menu allows the user to view the Switch history. This works like a trap and event receiver except it only captures trap/events generated by the Switch itself. For example, the switch history includes when the system is rebooted, when a console session is timed out, when a new link is established, and when configuration is save to flash memory.

To display the **Switch History** screen, choose **Network Monitoring** from the main menu and then choose **Switch History**. The following screen appears:

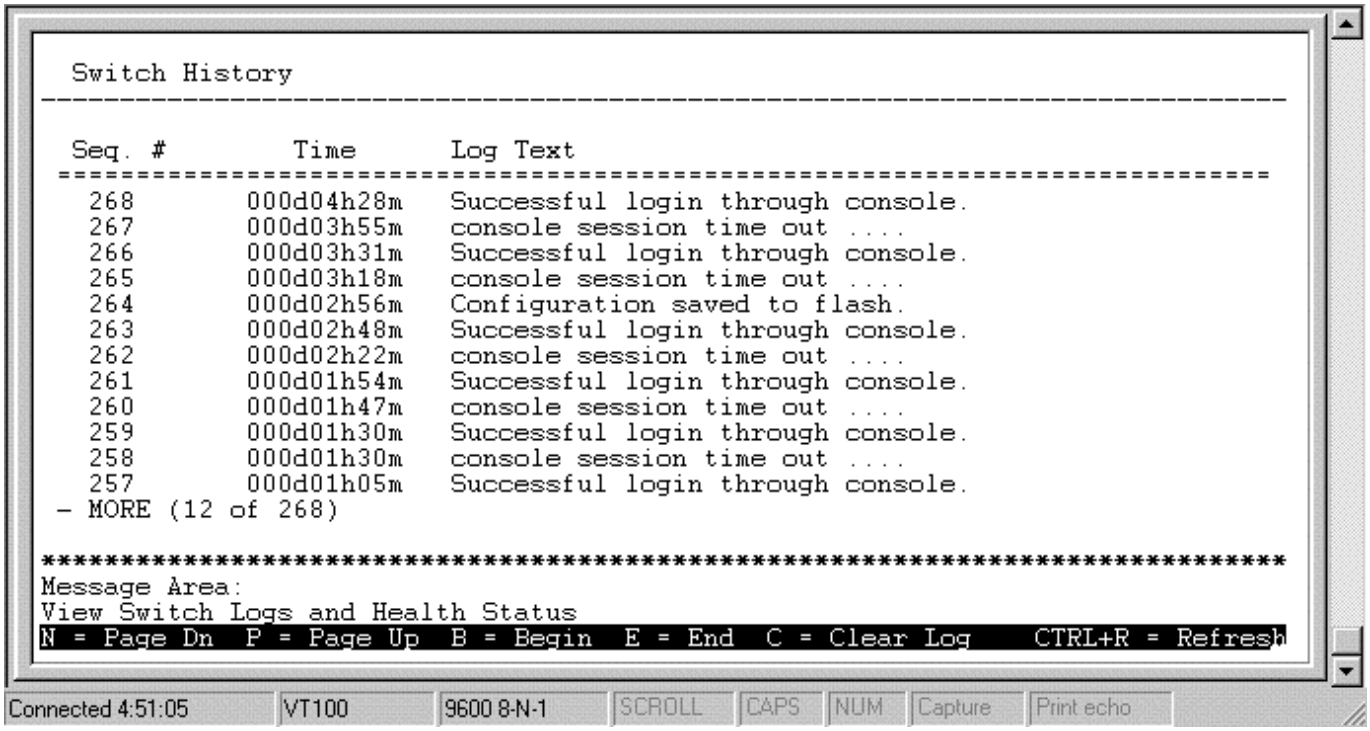

Switch History
Seq. # Time Log Text
268 000d04h28m Successful login through console.
267 000d03h55m console session time out ....
266 000d03h31m Successful login through console.
265 000d03h18m console session time out ....
264 000d02h56m Configuration saved to flash.
263 000d02h48m Successful login through console.
262 000d02h22m console session time out ....
261 000d01h54m Successful login through console.
260 000d01h47m console session time out ....
259 000d01h30m Successful login through console.
258 000d01h30m console session time out ....
257 000d01h05m Successful login through console.
- MORE (12 of 268)
Message Area:
View Switch Logs and Health Status
N = Page Dn P = Page Up B = Begin E = End C = Clear Log CTRL+R = Refresh
Connected 4:51:05
VT100
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 6-64. Switch History screen

The switch history entries are listed sequentially from the last time the Switch was rebooted. Use the following keys to move around the screen above: N – Page down, P – Page up, B – Begin, E – End, and C – Clear Log. CTRL+R will refresh the screen.

Resetting the Switch

You can use the console interface to reset the Switch, either performing a **Restart System** (which restarts the Switch and is identical to powering the Switch off and on again), or a **Factory Reset** (which sets all of the Switch's parameters to what they were when the Switch was purchased).

Restart System

To perform a system reset, choose **Restart System** from the main menu--a confirmation query will be offered before the system is rebooted.

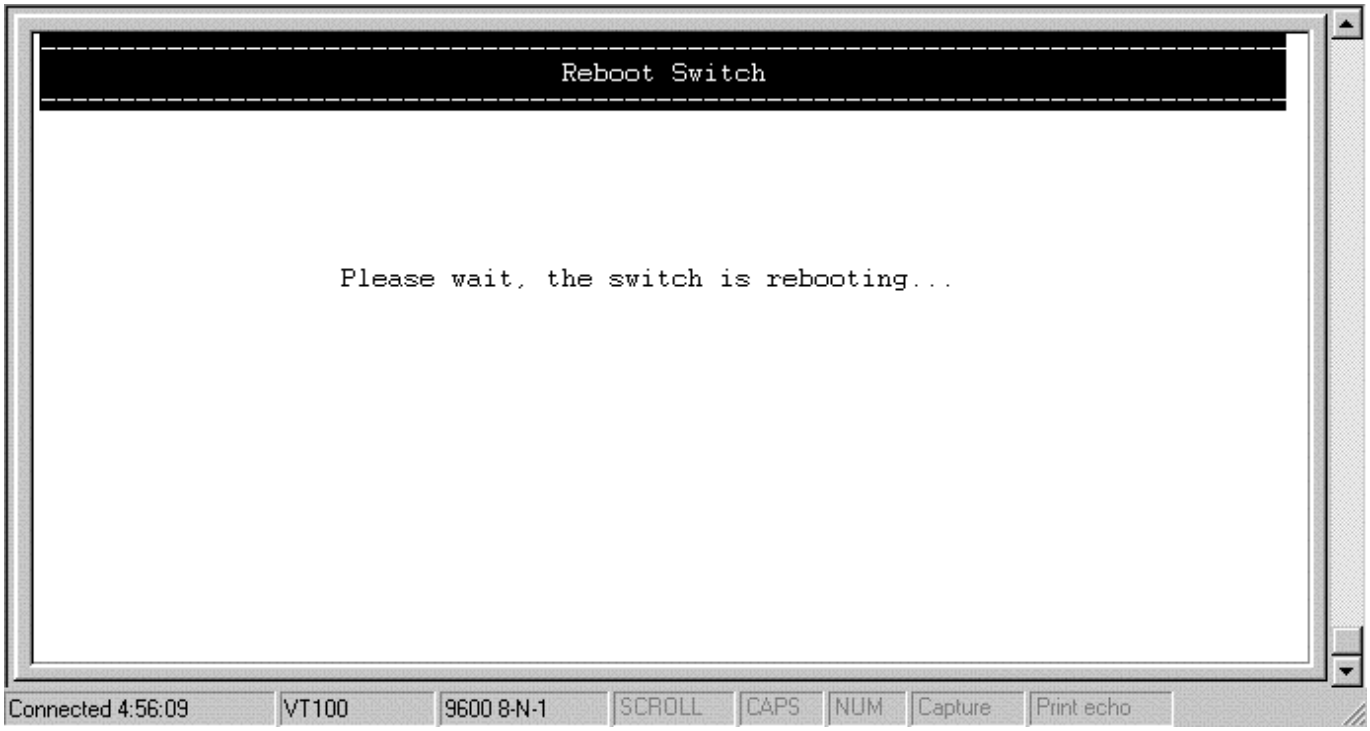


Figure 6-65. Restart System screen

Factory Reset

Before performing a factory reset, be absolutely certain that this is what you want to do. Once the factory reset is done, all of the Switch's settings stored in NV-RAM (including TCP/IP parameters, SNMP parameters, the enabled/disabled settings of ports, security settings, etc.) will be erased and restored to values present when the switch was purchased.

After performing the factory reset, make sure to redefine the IP settings for the Switch in the **Configure IP Address** menu. Then perform a **Restart System** on the Switch. After these three procedures are performed, your factory reset is complete.

Choose **Factory Reset** from the main menu. The following screen appears:

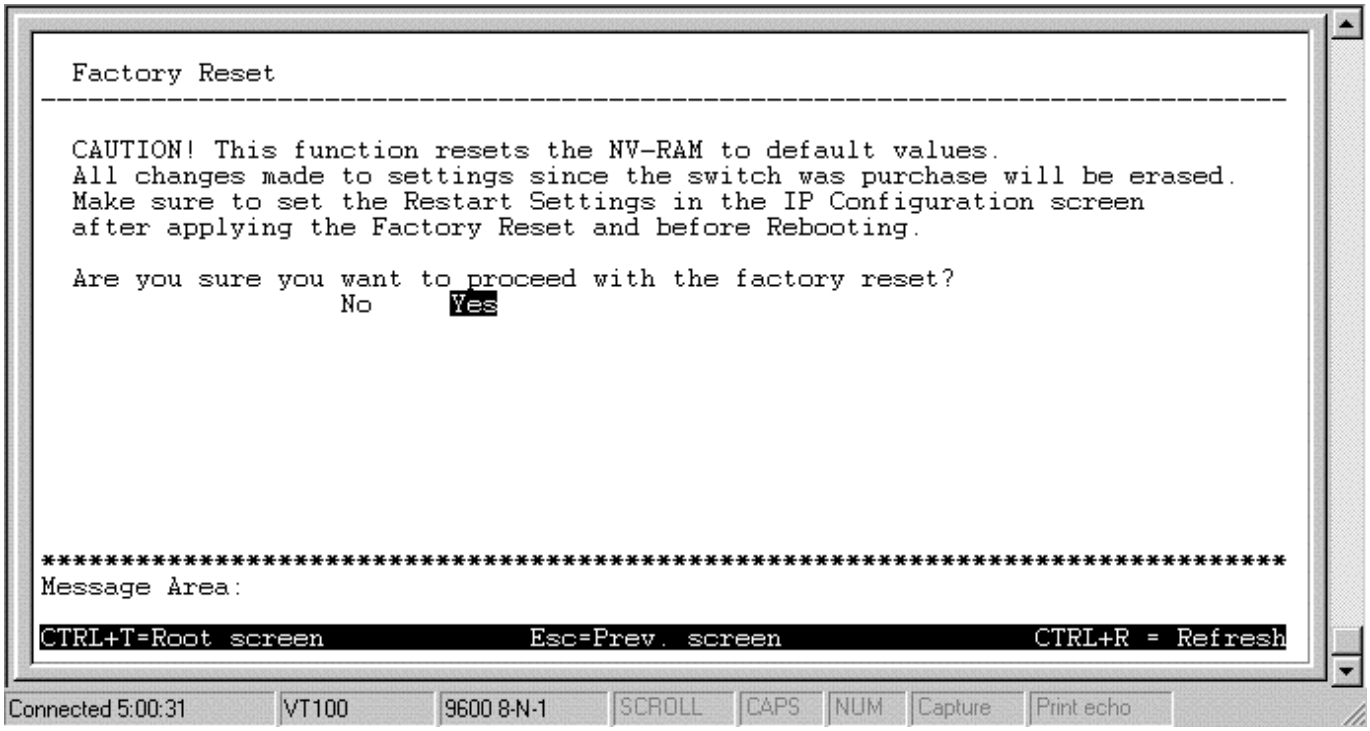


Figure 6-66. Factory Reset

Logout

To exit the console program, choose **Logout** from the main menu. Make sure you have performed a **Save Changes** if you have made changes to the settings and wish them to become defaults for the Switch. After logging out, you will be returned to the opening login screen.

7

WEB-BASED NETWORK MANAGEMENT

Introduction

The DES-3225G offers an embedded Web-based (HTML) interface allowing users to manage the Switch from anywhere on the network through a standard browser, such as Netscape Navigator/ Communicator or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol. Your browser window may vary with the screen shots (pictures) in this guide.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in Web-based management are the same as those found in the console program.

Note: This Web-based Management Module does not accept Chinese language input (or other languages requiring 2 bytes per character).

Getting Started

The first step in getting started in using Web-based management for your Switch is to secure a browser. A Web browser is a program which allows a person to read hypertext, for example, Netscape Navigator or Microsoft Internet Explorer. Follow the installation instructions for the browser.

The second and last step is to configure the IP interface of the Switch. This should be done manually through a console (see the *Configure IP Address* section in the *"Using The Console Interface"* chapter).

Management

To begin managing your Switch simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the switch.

In the page that opens, click on the **Login to DES-3225G Web-based Management** button:

This opens the main page in the management module.

The top of the main page has a button labeled **Click Here to Load Panel**:

Clicking on this button causes an interactive view of the Switch's front panel to be shown in the top portion of the window.

Clicking on one of the Ports opens a configuration window for that particular port.

The main page contains a list of buttons along the top of it labeled: **Configure Switch**, **Configure Management, Monitor**, **Reset and Update**, **Save Changes**, and **Help**. These are the major categories for Switch management. Clicking on one of the first four categories causes a list of options to appear in the left panel of the main window.

The switch management features available in the Web-based are explained below.

Configure Switch

This first category includes: **IP Settings**, **Port Settings**, **Port Mirroring**, **Switch Settings** (**Basic** and **Advanced**), **Filtering and Forwarding Table** (**Configure**, **Static Forwarding Table**, **MAC Address Filtering**, and **Static Multicast Forwarding**), **Spanning Tree** (**STP Parameter** and **STP Parameter & Port Settings**), **IGMP Filtering** (**IGMP Settings** and **Configure 802.1Q IGMP**), **VLANs & MAC-based Broadcast Domains** (**Configure VLANs & MAC-based Broadcast Domains**, **Configure IEEE 802.1Q VLANs**, and **Configure GMRP**), and **Trunk**, as well as a number of related windows.

IP Settings

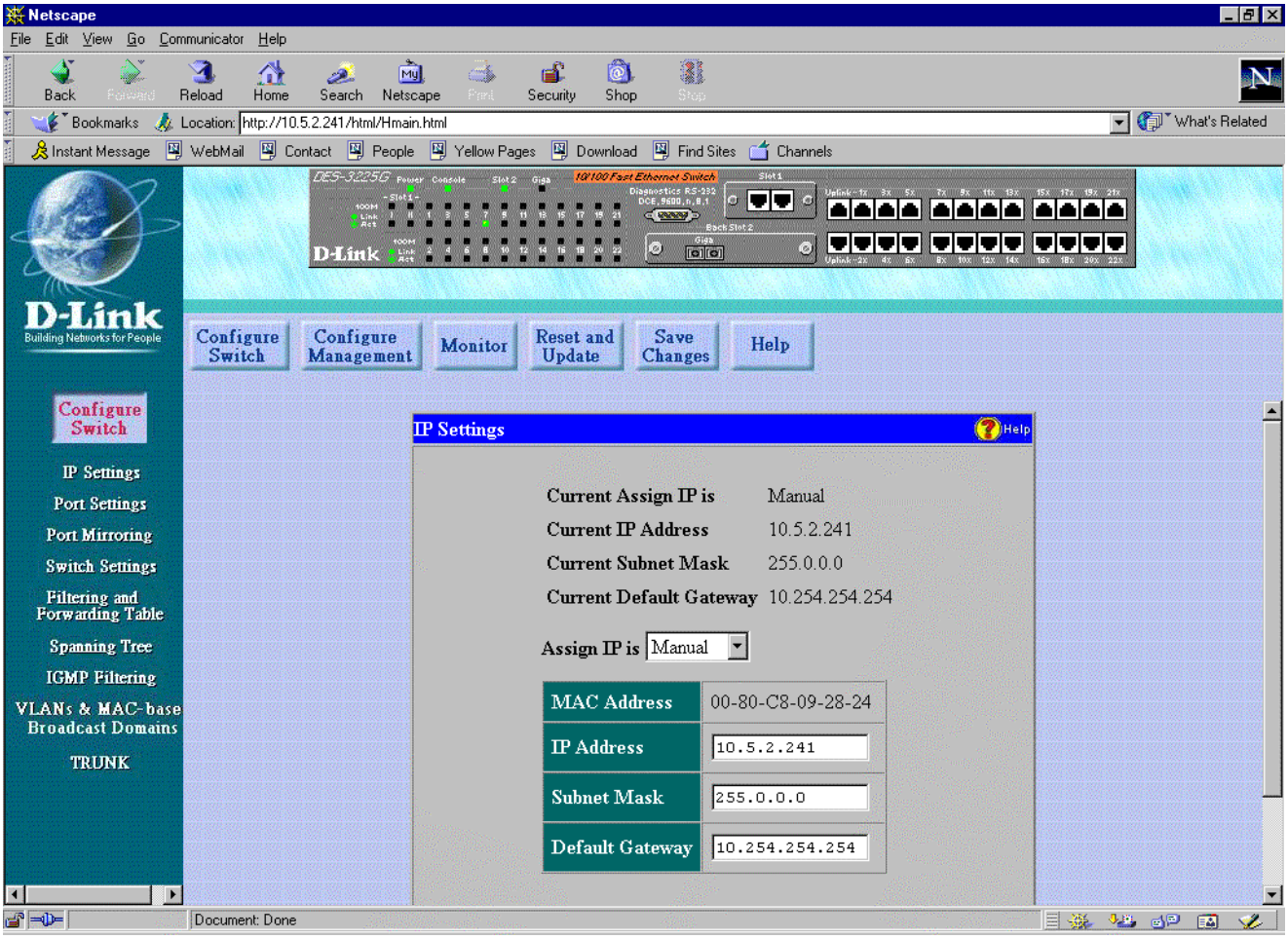


Figure 7-1. IP Settings window

This window is used to determine whether the Switch should get its IP Address settings from the user (*Manual*), a *BOOTP* server, or a *DHCP* server. If you are not using either BOOTP or DHCP, enter the **IP Address**, **Subnet Mask**, and **Default Gateway** of the Switch. If you enable BOOTP, you do not need to configure any IP parameters because a BOOTP server automatically assigns IP configuration parameters to the Switch. If you enable DHCP, a Dynamic Host Configuration Protocol request will be sent when the Switch is powered up. Once you have selected a setting under Assign IP is, click **Apply** to activate the new settings.

The information is described as follows:

- **Assign IP is** There are three choices for how the Switch receives its IP Address settings: *Manual*, *BOOTP*, and *DHCP*.
- **MAC Address** The Ethernet address for the device. Also known as the physical address
- **IP Address** The host address for the device on the TCP/IP network.
- **Subnet Mask** The address mask that controls subnetting on your TCP/IP network.
- **Default Gateway** The IP address of the device, usually a router, that handles connections to other subnets and/or other TCP/IP networks.

Port Settings

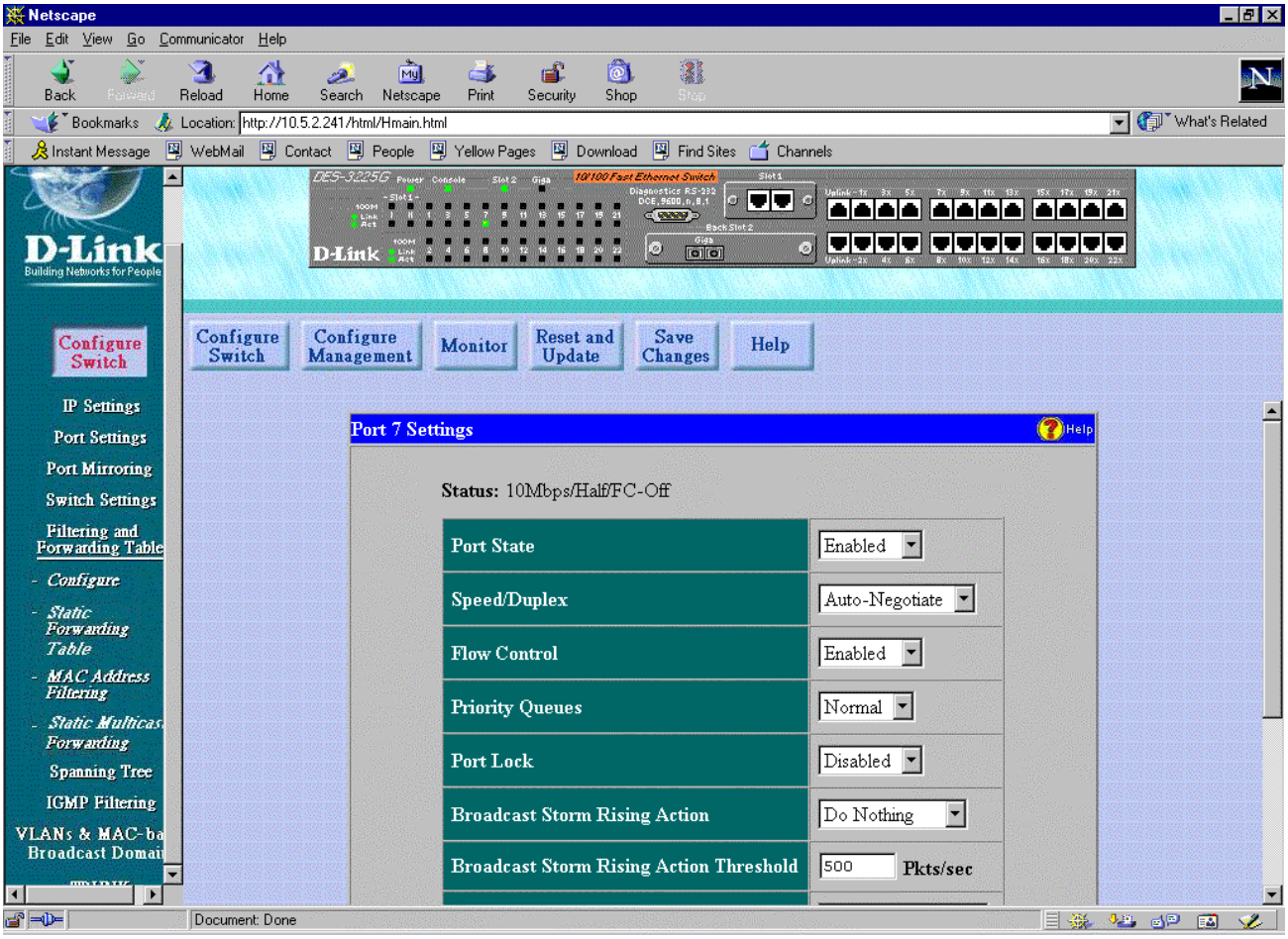


Figure 7-2. Port Settings window

Select the port you want to configure by clicking on the port in the Switch front panel display at the top of the window. Follow these steps:

1. Enable or disable the port. If you choose *Disabled*, devices connected to that port cannot use the Switch, and the Switch purges their addresses from its address table after the MAC address aging time elapses. The Switch won't purge addresses if you define them as permanent entries in the **MAC Forwarding Table**.

2. Configure the **Speed/Duplex** setting for the port. Select *Auto-Negotiate* to allow the port to select the best transmission speed, duplex mode and flow control settings based on the capabilities of the device at the other end. The other selections allow you to force the port to operate in the specified manner. Select *100Mbps/Full* for port operation at 100 Mbps and full duplex. Select *100Mbps/Half* for port operation at 100 Mbps and half duplex. Select *10Mbps/Full* for port operation at 10 Mbps and full duplex. Select *10Mbps/Half* for port operation at 10 Mbps and half duplex.

3. Configure the **Flow Control** setting for the port. Selecting *Enabled* in full-duplex mode will implement IEEE 802.3x flow control. Selecting *Enabled* when the port is in half-duplex mode will implement normal Ethernet collision-based backpressure flow control. Select *Disabled* for no flow control. Also, if the port is set for *Auto* (NWay) in the speed/duplex field above and flow control is enabled, flow control (whether full- or half-duplex) will only be implemented if the other device can auto-negotiate flow control. Note that you must reboot the Switch before a flow control change can take effect.

4. Configure the **Priority Queues** setting for packets passing through this port, using IEEE 802.1 tagging. Select *Low*, *High* or *Normal*. If the network is congested, the Switch handles packets with a higher priority before those with lower priority.

5. Configure the **Port Lock** setting to prevent the port from learning MAC addresses of new hosts. This will help keep intruders off your network since any packet coming from an unknown source will be dropped by the Switch, that is, not added to your MAC Address Forwarding Table. Select *Enabled* or *Disabled*.

6. Configure the **Broadcast Storm Rising Action** setting from three choices: *Do Nothing*, *Blocking*, or *Blocking-Trap* and the **Broadcast Storm Rising Action Threshold** that will trigger a Broadcast Storm Rising Action.

7. Configure the **Broadcast Storm Falling Action** setting from three choices: *Do Nothing*, *Forwarding*, or *Forwarding-Trap* and the **Broadcast Storm Falling Action Threshold** that will trigger a Broadcast Storm Falling Action.

8. The **STP Port State** read-only field indicates the status of the Spanning Tree Protocol, e.g. *Forwarding*.

9. Click **Apply** to let your changes take effect.

To see all the ports on the Switch rather than just an individual port, click **View All Ports** at the bottom of the window.

Port Mirroring

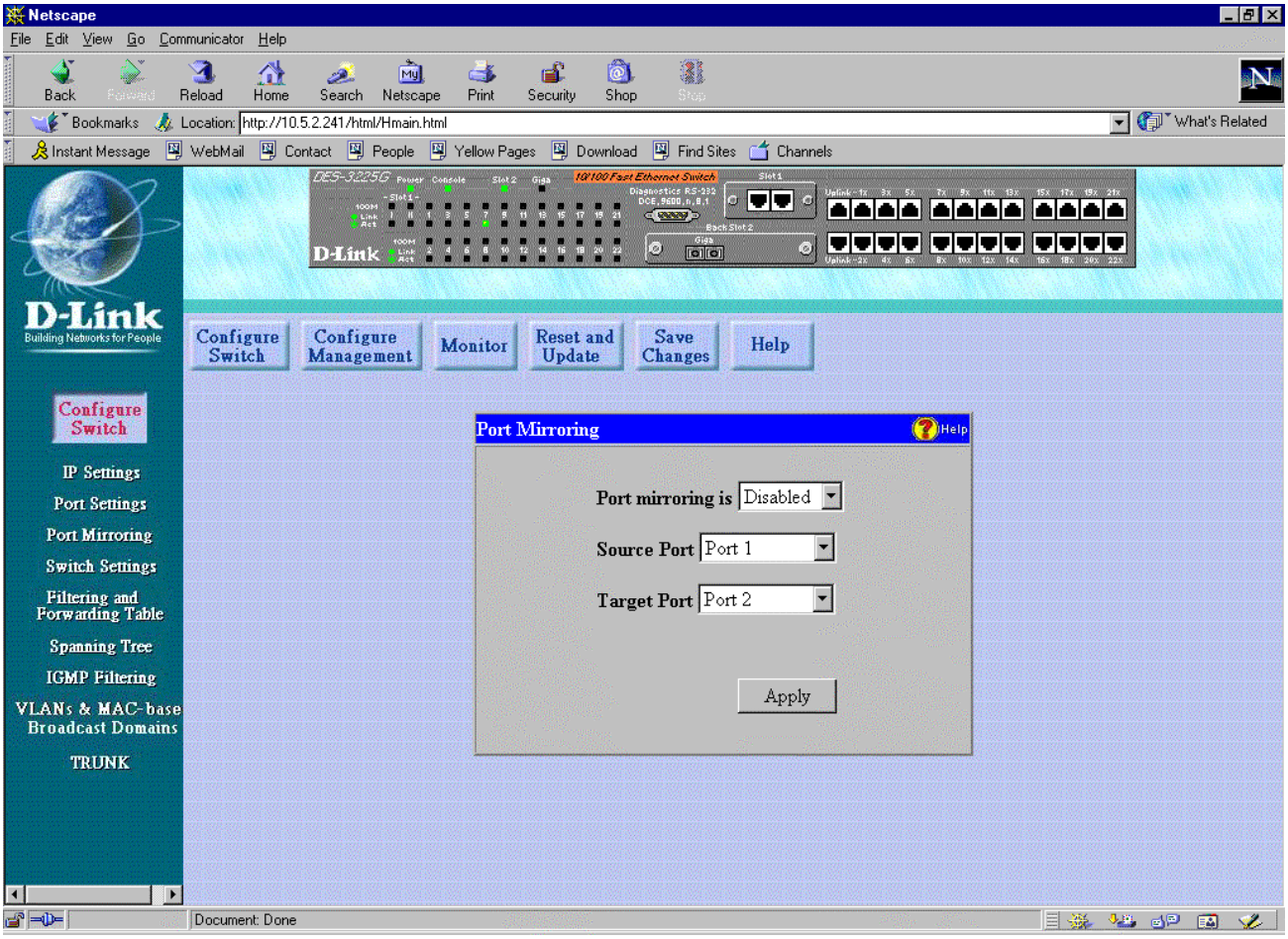


Figure 7-3. Port Mirroring window

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port.

To configure a mirror port, select *Enabled* from the **Port mirroring in** pull-down list. In the next field, select the **Source Port** from where you want to copy frames. In the last field, select the **Target Port**, which receives the copies from the source port. This is the port where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe. Click **Apply** to let the changes take effect.

Note: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port can not be the same port.

Switch Settings

Basic

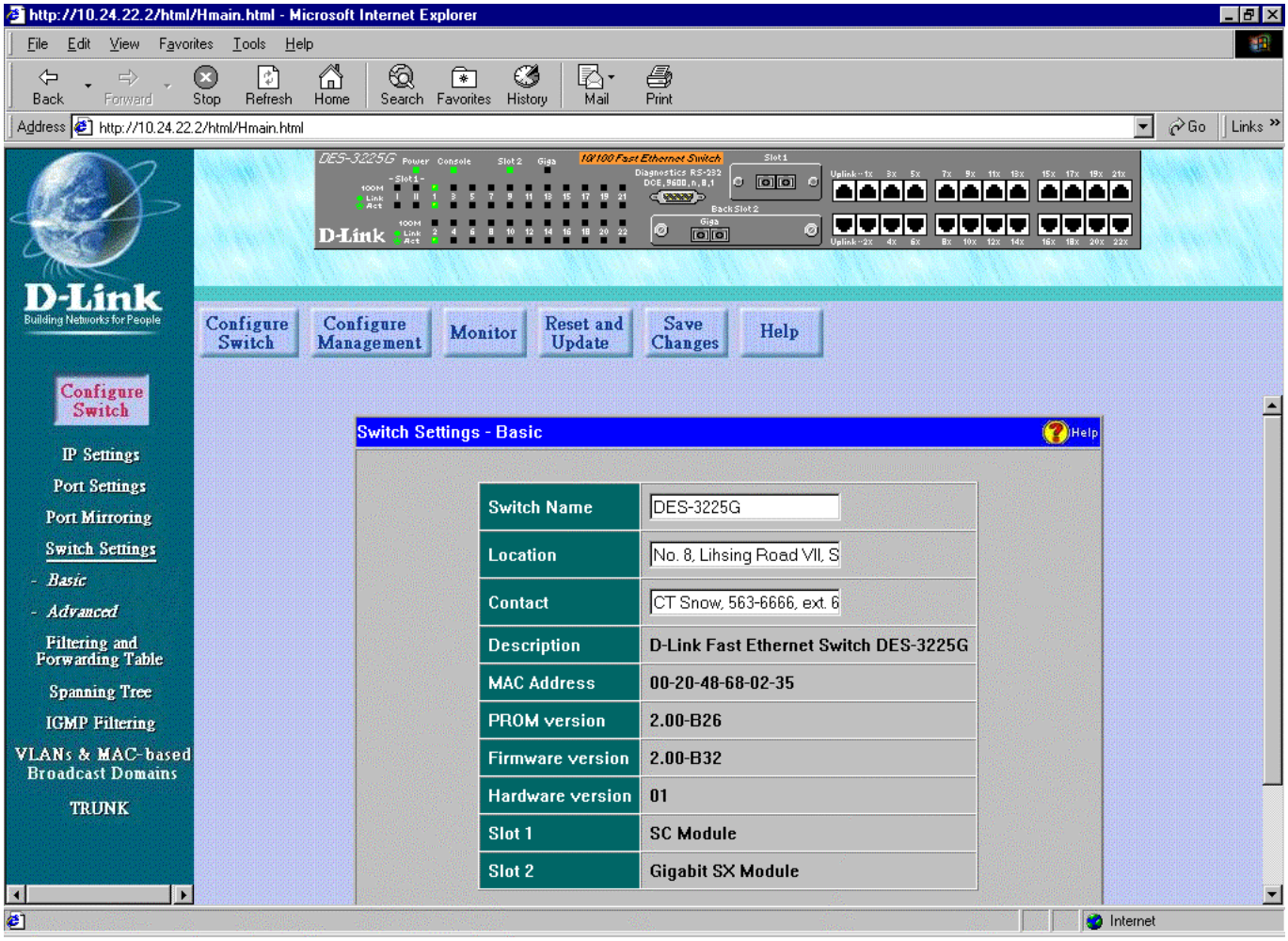


Figure 7-4. Switch Settings - Basic window

To set basic switch settings, enter a **Switch Name** in the first field, the physical location of the Switch in the **Location** field, and the name of the contact person responsible for the Switch in the **Contact** field. Then click **Apply**.

The information is described as follows:

- **Switch Name** A user-assigned name for the Switch.
- **Location** A user-assigned description for the physical location of the Switch.
- **Contact** Name of the person to contact should there be any problems or questions with the system. You may also want to include a phone number or extension.
- **Description** A description of the Switch type.
- **MAC Address** The Ethernet address for the device.
- **PROM version** Version number for the firmware chip. This information is needed for new runtime software downloads.

- **Firmware version** Version number of the firmware installed on the Switch. This can be updated by using the **Update Firmware** window in the **Reset and Update** section.
- **Hardware version** Version number of the Switch's hardware.
- **Slot 1** Description of module plugged into slot 1, located on the front-of the Switch.
- **Slot 2** Description of module plugged into slot 2, located on the rear of the Switch.

Advanced

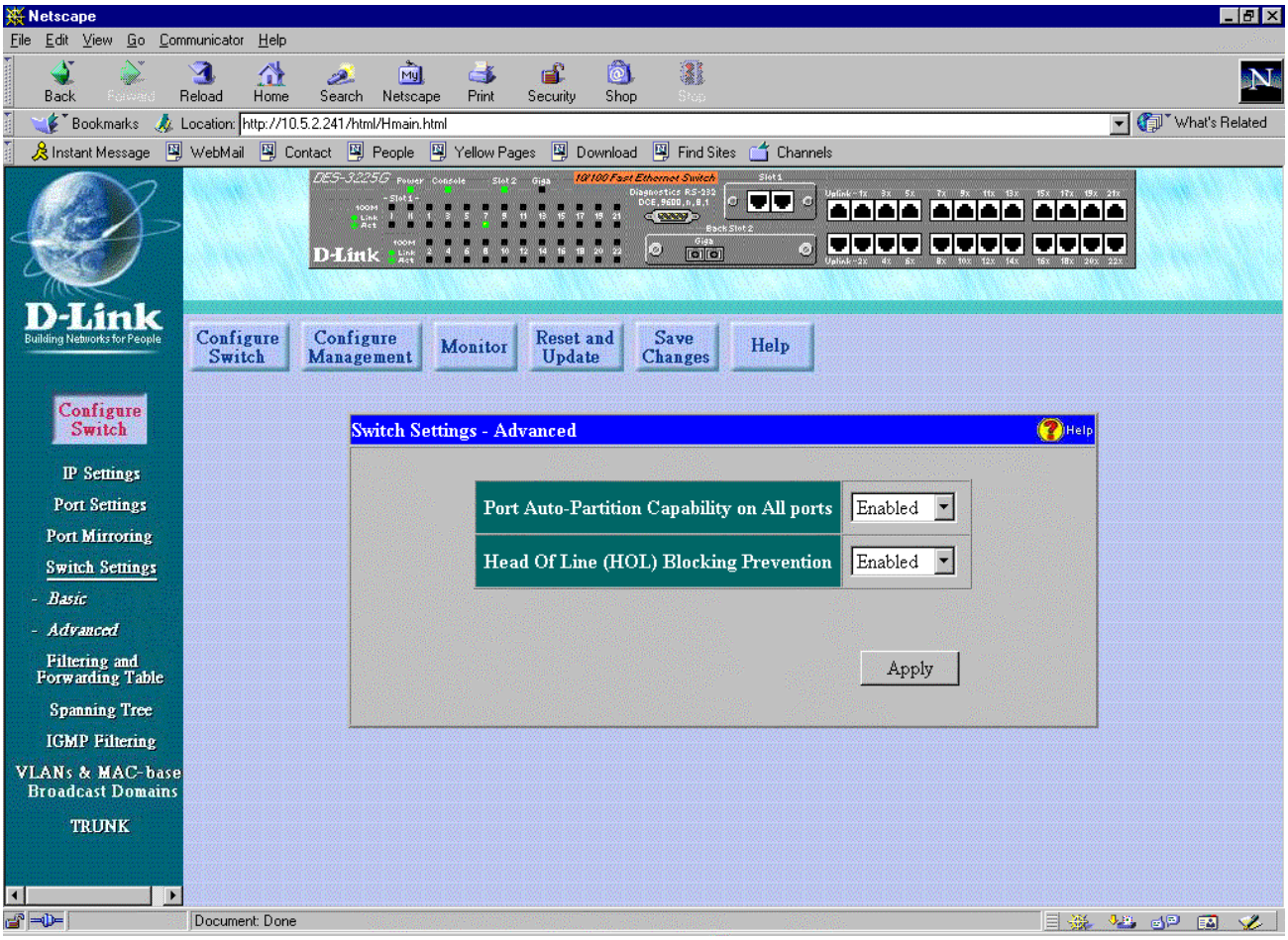


Figure 7-5. Switch Settings - Advanced window

The first setting allows you to enable or disable port auto-partitioning by the **Port Auto-Partition Capability on All ports** function. If you enable auto-partitioning on all ports, when more than 63 collisions occur while a port is transmitting data, the port automatically stops transmissions. The second setting allows you to enable or disable the **Head of Line (HOL) Blocking Prevention** function, which is designed to prevent forwarding a packet to a "blocking" port. Click **Apply** to let your changes take effect.

The information in the window is described as follows:

- **Port Auto-Partition Capability on All ports** This option offers *Enabled* or *Disabled* to decide whether to auto-partition a selected port and take it offline or not.
- **Head of Line (HOL) Blocking Prevention** This option prevents forwarding a packet to a port where an excess of packets are queued up. Note that when a multicast packet or a packet with an unknown destination address needs to be forwarded to several ports, and if some of them are

"blocking," the packet will not be discarded, rather it will be forwarded only to the ports that are not "blocking."

Filtering and Forwarding Table

When a packet hits the Switch, it looks in the filtering and forwarding table to decide what to do with the packet; either to filter it off the network, or to forward it through the port on which its destination lies.

Configure

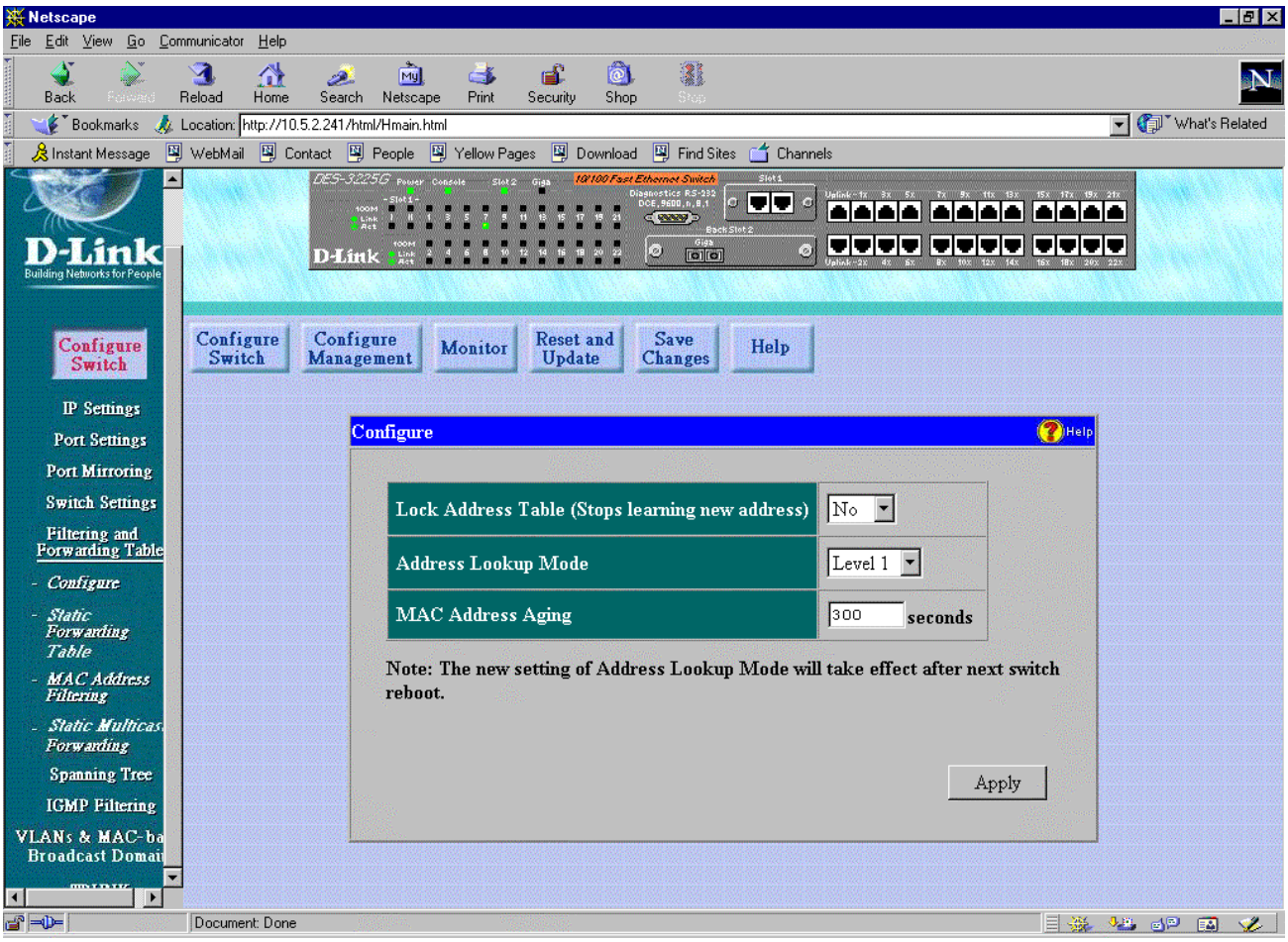


Figure 7-6. Configure window

This window allows you to stop or start address learning, use an address look-up mode, and select an age-out time of the MAC address in the selected address table. Click **Apply** to let your changes take effect.

The following fields above can be set:

- **Lock Address Table (Stops learning new address)** Mostly used for security purposes, when the forwarding table is locked the Switch will no longer learn the MAC addresses for new hosts. If your network configuration doesn't change, locking the forwarding table helps keep intruders off your network since any packet coming from an unknown source address will be dropped by the Switch.
- **Address Look-up Mode** Select from: *Level 0*, *Level 1*, *Level 2*, *Level 3*, *Level 4*, *Level 5*, *Level 6*, or *Level 7*. Reboot the Switch to allow the new setting to take effect.
- **MAC Address Aging** Enter the desired MAC address age-out time in this field (10 to 1000000 seconds).

Static Forwarding Table

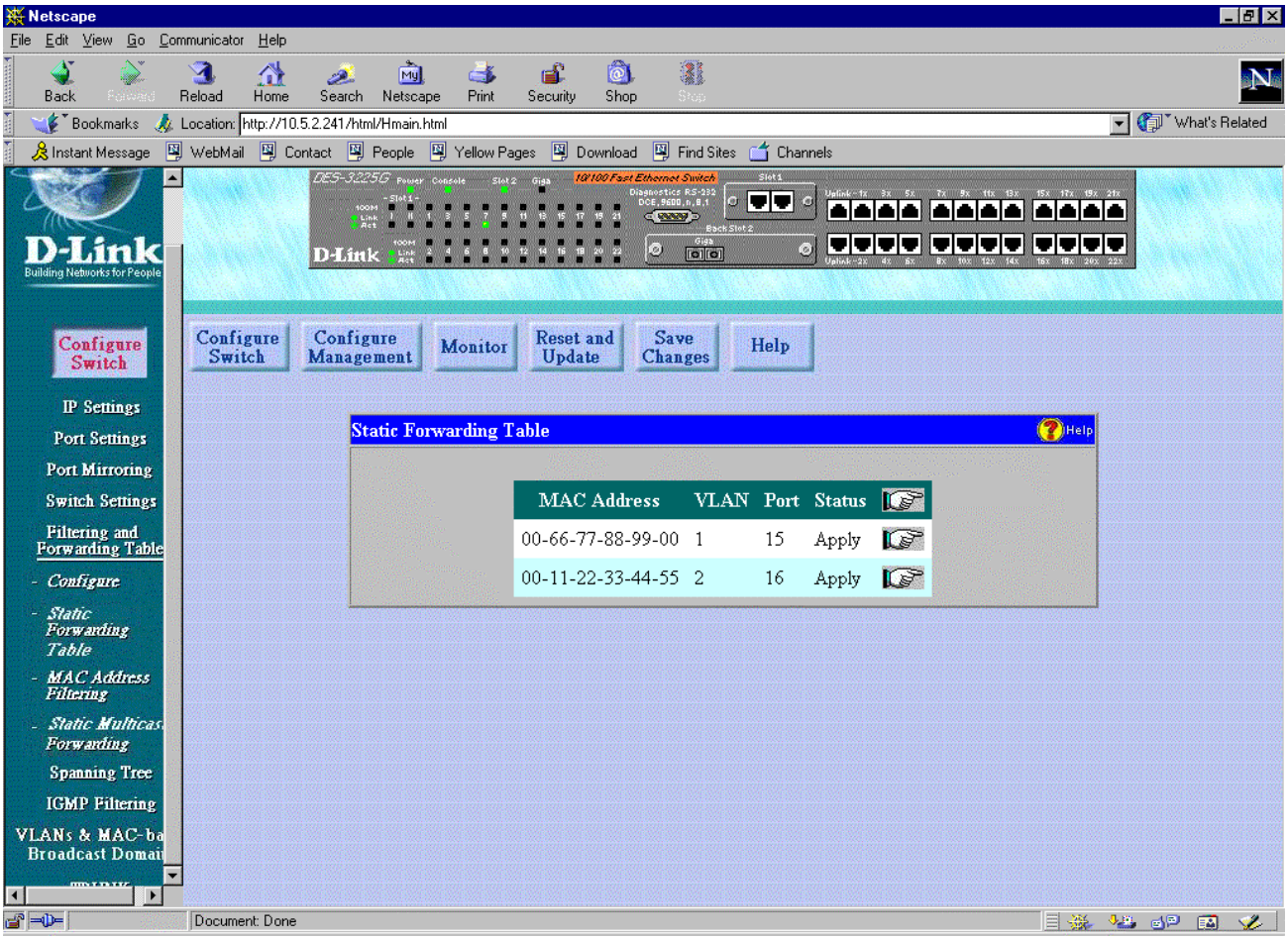


Figure 7-7. Static Forwarding Table window

Static forwarding allows the Switch to permanently forward outbound traffic to specific destination MAC addresses over a specified port.

Click the pointer icon on the right side of the table to access the **Add/Modify Static Forwarding Table Entry** window:

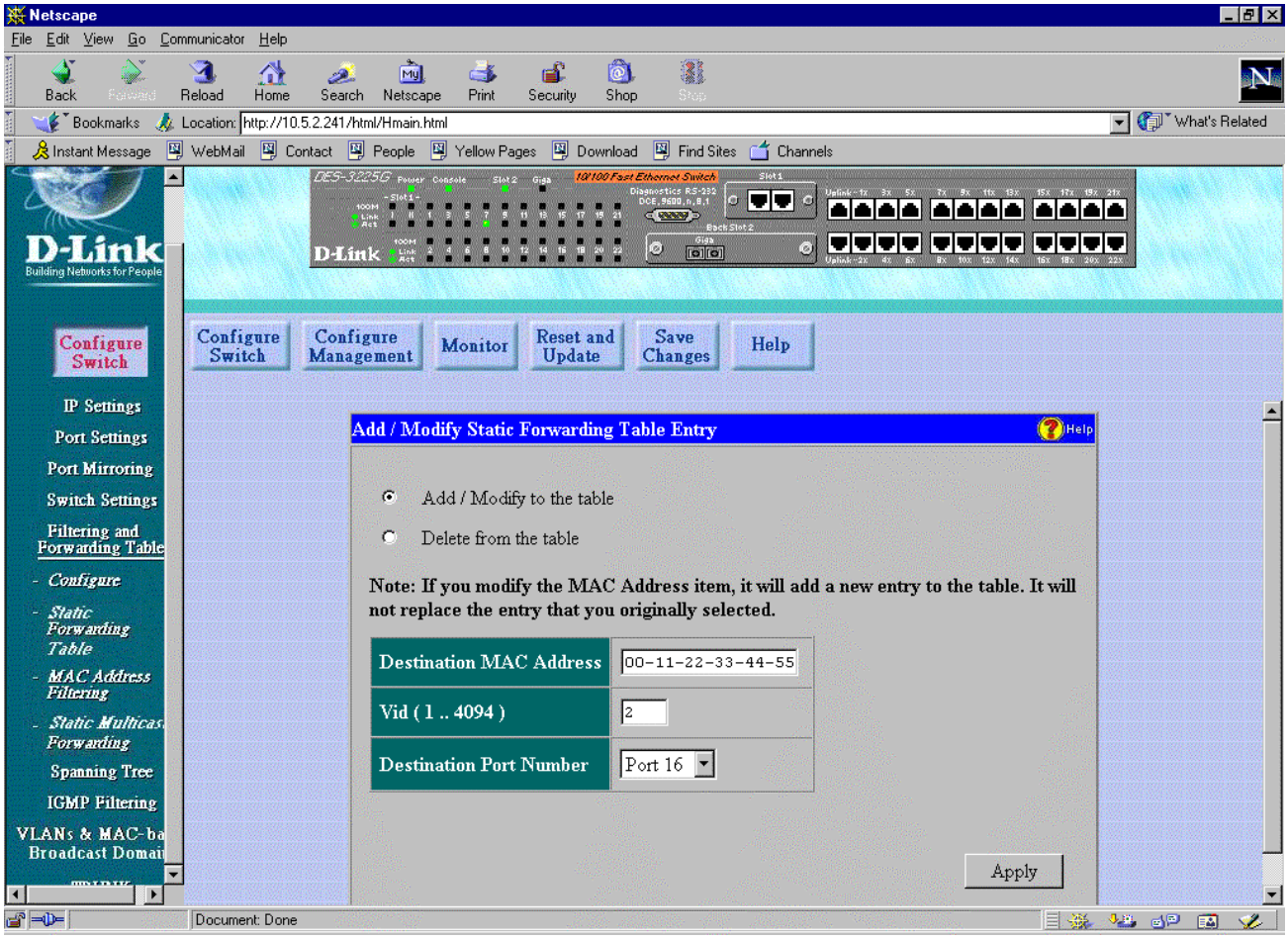


Figure 7-8. Add/Modify Static Forwarding Table Entry window

To use the static forwarding function, check either the **Add/Modify to the table** option button or the **Delete from the table** option button, enter the MAC address of the device to which the specified port permanently forwards traffic in the **Destination MAC Address** field, enter a VLAN ID number in the second field, and enter the port number that permanently forwards traffic from the specified device in the **Destination Port Number** field. Then click **Apply**.

The information in the window is described as follows:

- **Add/Modify to the table/Delete from the table** Choose one of the desired options to add/modify or delete an entry from the table.
- **Destination MAC Address** The MAC address of the device to which the specified port permanently forwards traffic.
- **Vid (1 .. 4094)** This is the VLAN ID number for the VLAN that has an agent attached to it which enables IGMP packets to be sent and received.
- **Destination Port Number** The port number that permanently forwards traffic from the specified device, regardless of the device's network activity or current network congestion.

MAC Address Filtering

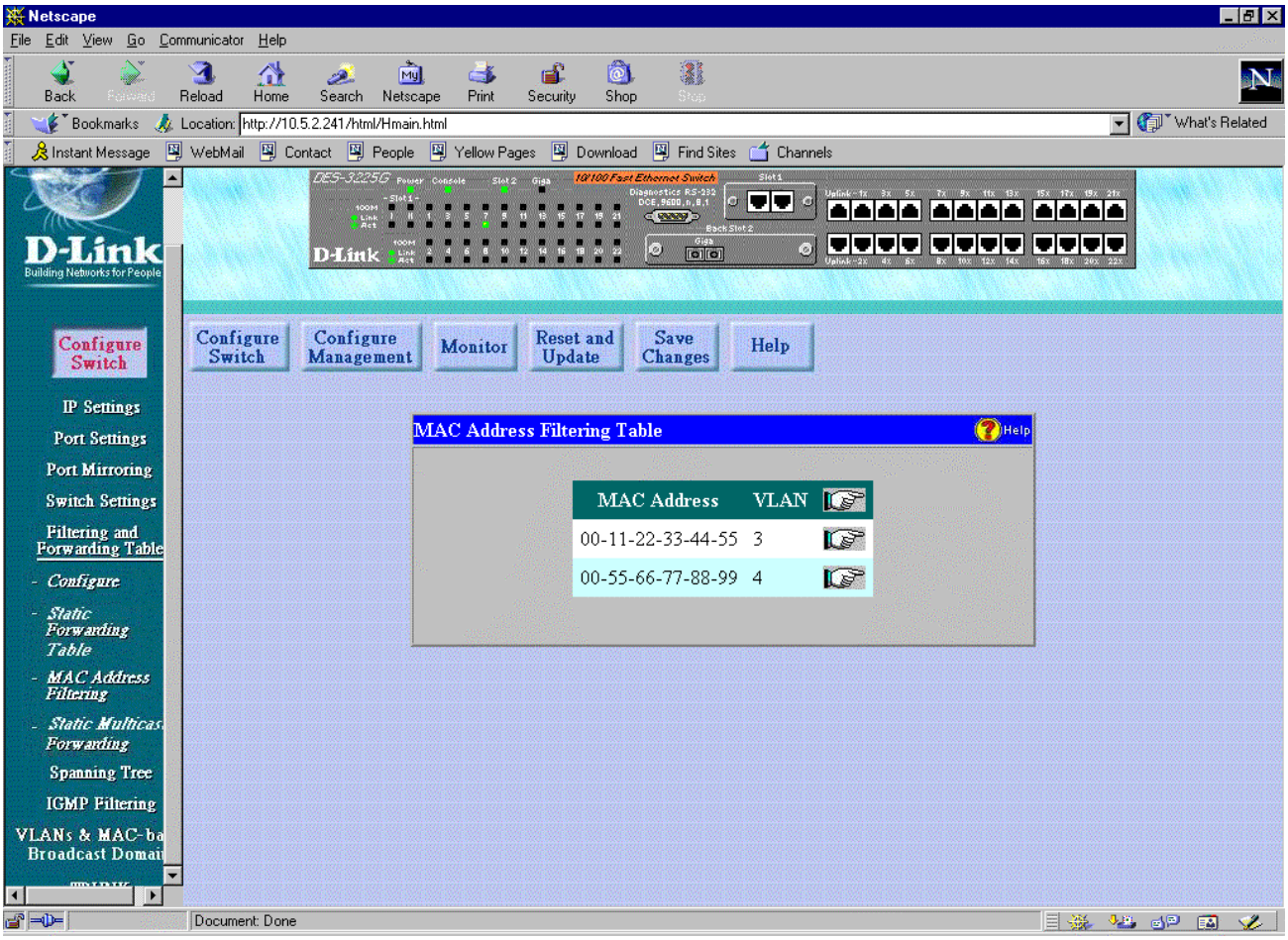


Figure 7-9. MAC Address Filtering Table window

MAC address filtering allows you to designate MAC addresses and VLANs which will be filtered from sending packets to the Switch. Please note that when a mode other than IEEE 802.1Q VLANs is selected, the only column that will appear on the table above is MAC Address.

Click the pointer icon on the right side of the table to access the **Add/Modify MAC Address Filtering Table Entry** window:

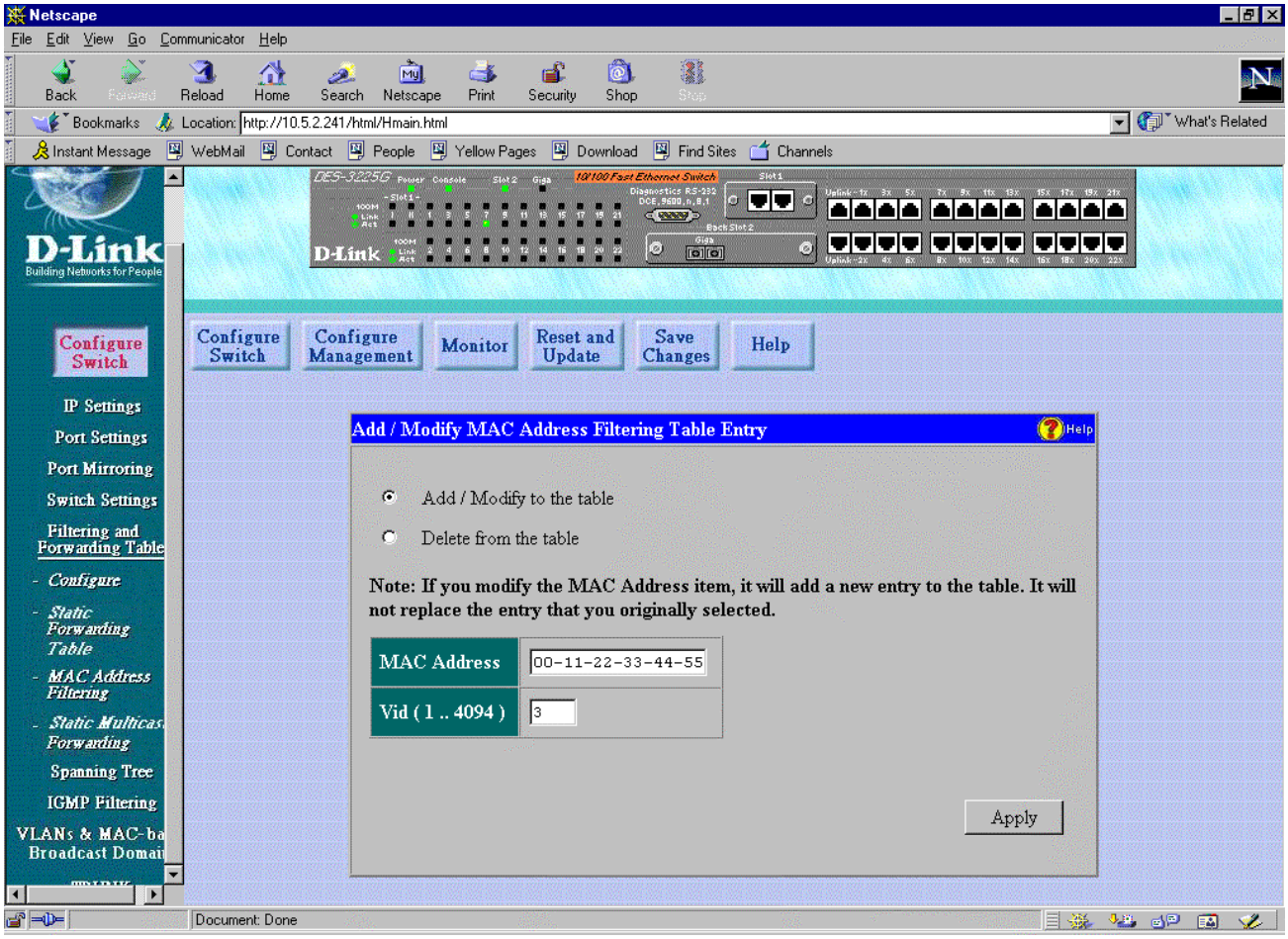


Figure 7-10. Add/Modify MAC Address Filtering Table Entry window

To use the MAC address filtering function, check either the **Add/Modify to the table** option button or the **Delete from the table** option button, enter the MAC address and the VLAN ID of the device being filtered in the two fields offered (the Vid (1..4094) field will only be displayed when the IEEE 802.1Q VLANs mode has been selected), and then click **Apply**.

The information above is described as follows:

- **Add/Modify to the table/Delete from the table** Choose one of the desired options to add, modify, or delete an entry from the **MAC Address Filtering Table**.
- **MAC Address** The Ethernet address of the **MAC Address Filtering Table** entry.
- **Vid (1 .. 4094)** This is the VLAN ID number for the VLAN that has an agent attached to it which enables IGMP packets to be sent and received.

Static Multicast Forwarding

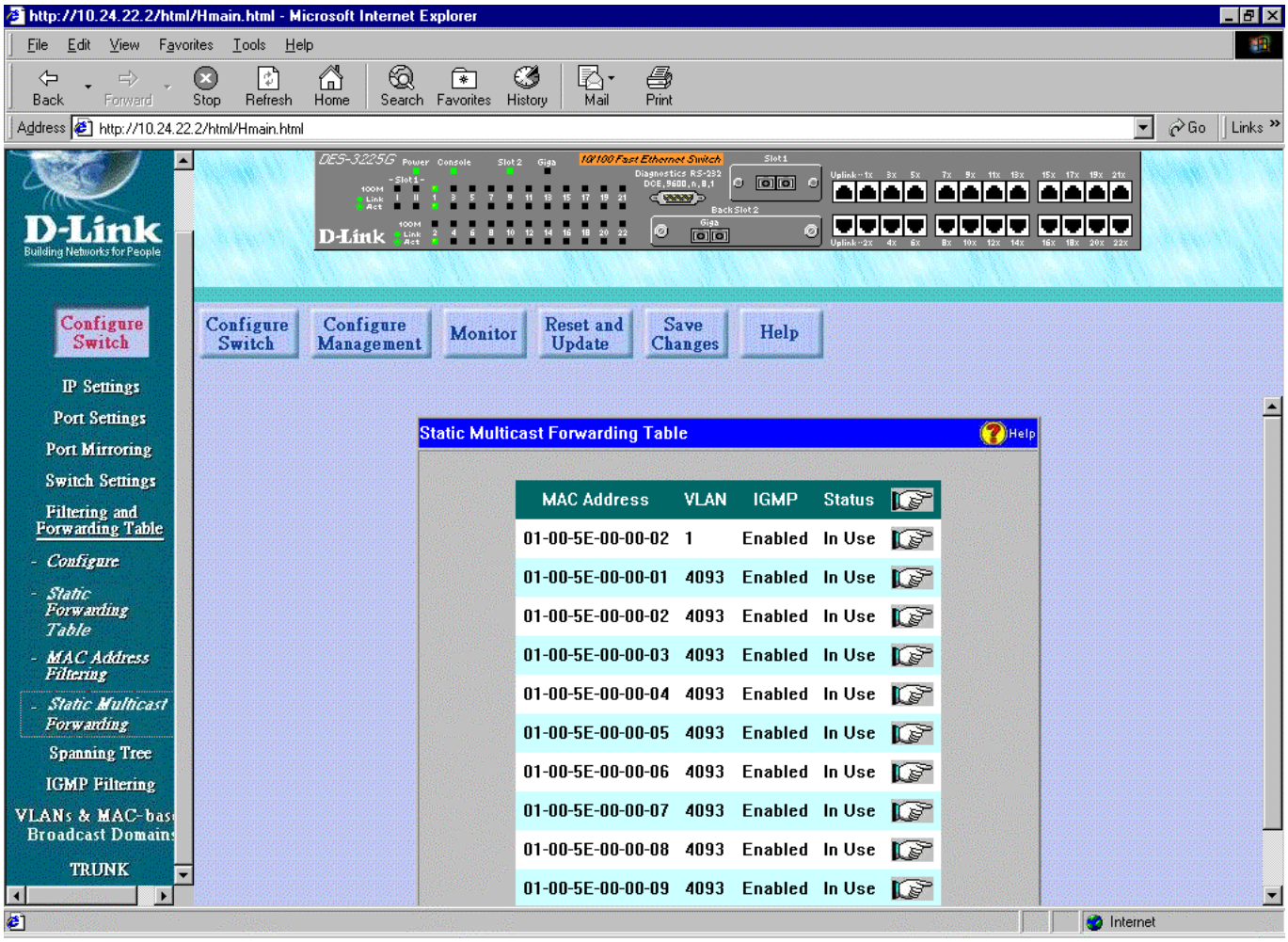


Figure 7-11. Static Multicast Forwarding Table window

This function forwards traffic over each port for one multicast group. You can configure each port on the Switch to forward traffic for the specified multicast group.

Click the pointer icon on the right side of the table to access the **Add / Modify Static Multicast Forwarding Table Entry** window shown below:

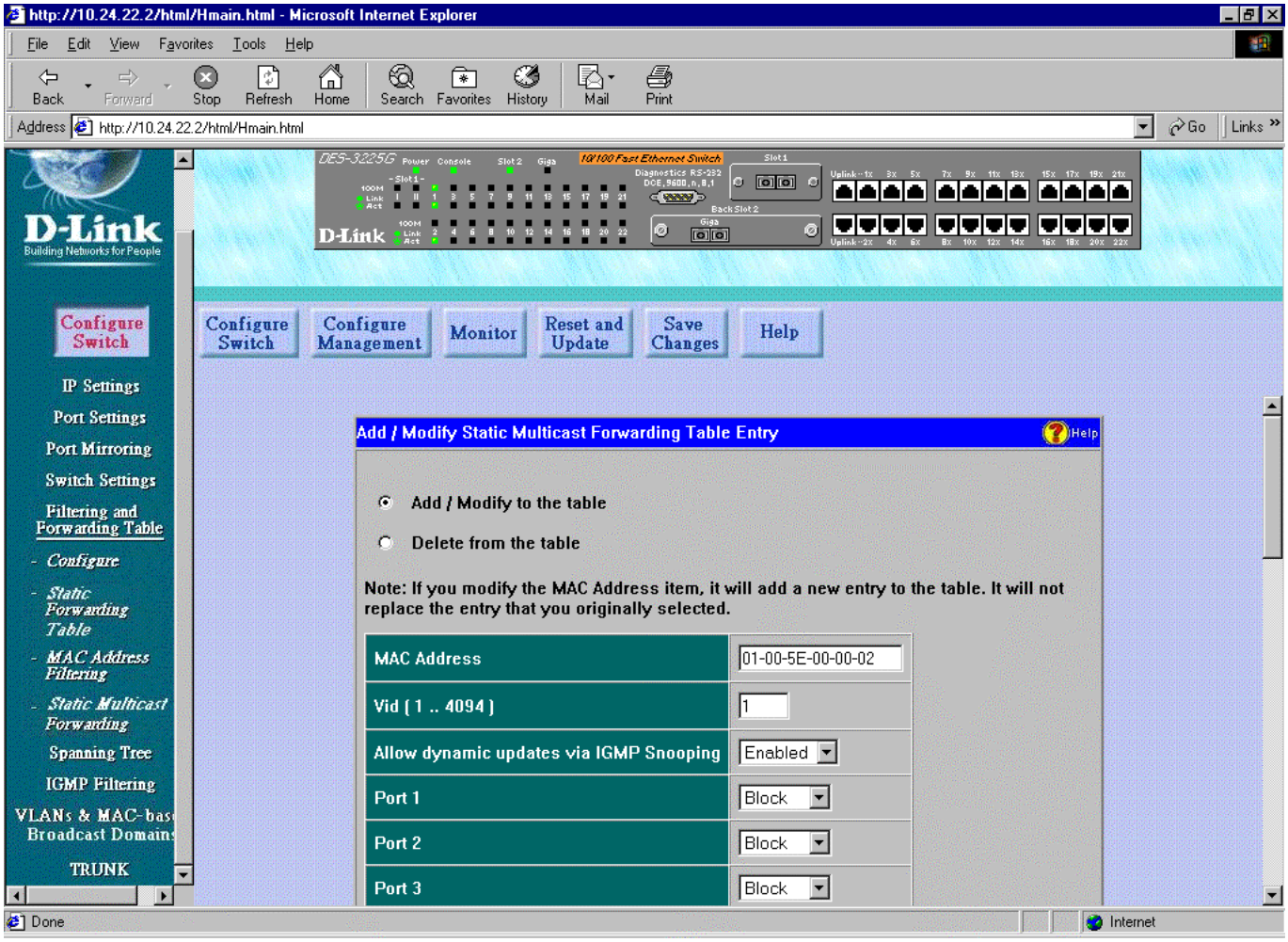


Figure 7-12. Add / Modify Static Multicast Forwarding Table Entry window

To **Add / Modify to the table** or **Delete from the table**, check the desired option button, enter the MAC address in the **MAC Address** field, enter the VLAN ID in the **Vid** field (if *IEEE 802.1Q VLANS* is selected), enable or disable the **Allow dynamic updates via IGMP Snooping** function, and select *Block* or *Forward* for each port. Click **Apply** to let the changes take effect.

The information above is described as follows:

- **Add/Modify to the table** Allows you to create or edit a filter for the **Static Multicast Forwarding Table** which will either forward or block multicast traffic.
- **Delete from the table** Allows you to delete a filter from the **Static Multicast Forwarding Table**.
- **MAC Address** The Ethernet address of the **Static Multicast Forwarding Table** entry. Only valid Multicast addresses will be added to the table.
- **Vid** This is the VLAN that will be defined on this screen. Note a VLAN ID is from 1 to 4094.
- **Allow dynamic updates via IGMP Snooping** Enable this function to tell the switch how to deal with the newly-created Static Multicast Forwarding table entry.
- **Port** Choose *Block* or *Forward* for each individual port.

Spanning Tree

The Switch supports 801.2d Spanning Tree Protocol, which allows you to create alternative paths (with multiple switches or other types of bridges) in your network. See the Spanning Tree Algorithm section of the "*Switch Management Concepts*" chapter for a detailed explanation.

STP Parameter

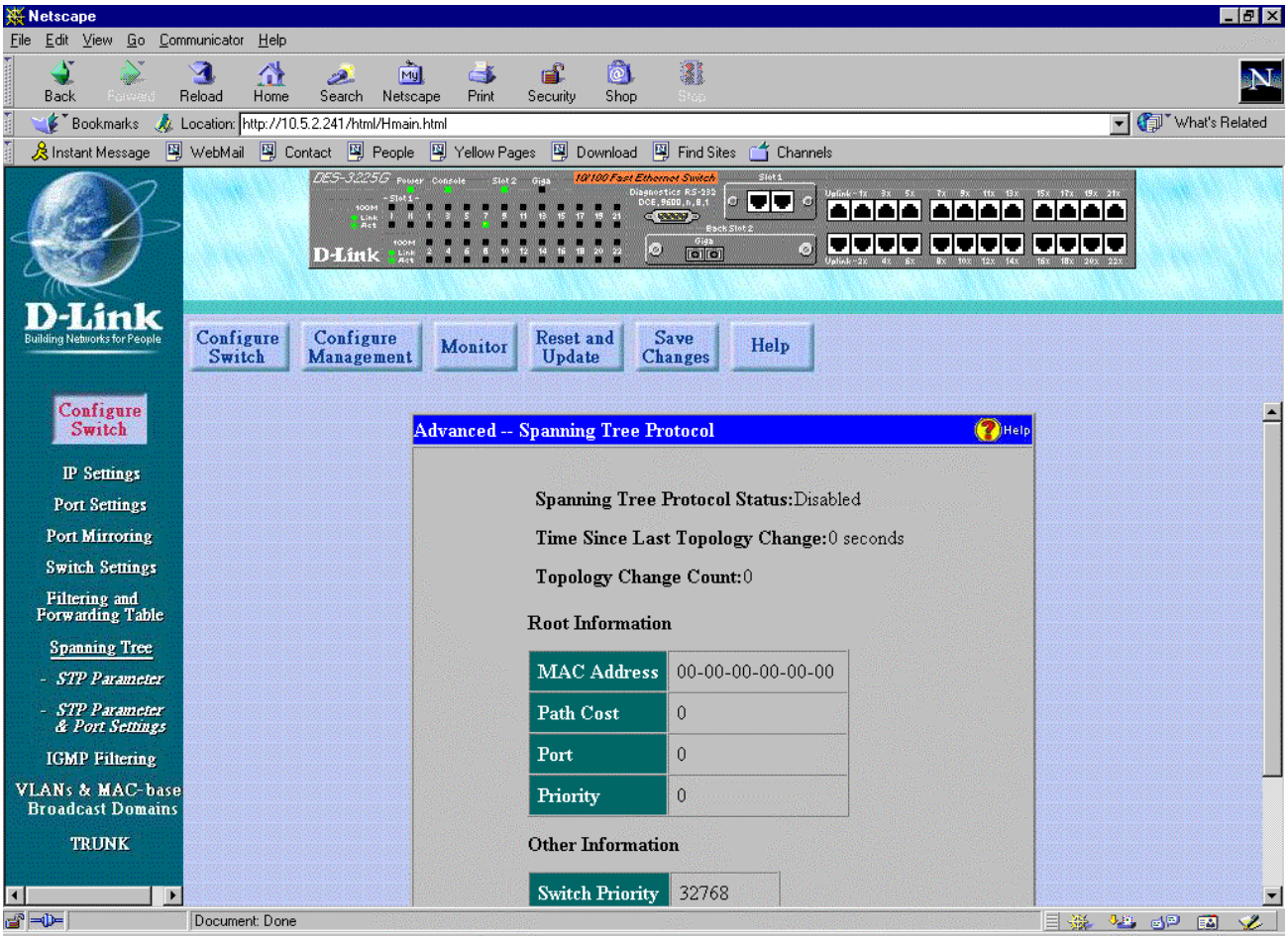


Figure 7-13. Advanced - Spanning Tree Protocol window

The information above is described as follows:

- **Spanning Tree Protocol Status** Displays the current Spanning Tree Protocol setting.
- **Time Since Last Topology Change** Displays the last time changes were made to the network topology. These changes usually occur when backup paths are activated due to primary path failures.
- **Topology Change Count** Displays the number of times (since the current management session with the device was started) changes were made to the network topology. Changes usually occur on the network when backup paths are activated.
- **MAC Address** Displays the MAC address of the switch acting as the root bridge.
- **Path Cost** Displays the cost for the path between the Switch and the root bridge. If the Switch is the root bridge, then the path cost is zero.

- **Port** Displays the port (on the switch) that offers the least path cost from the bridge to the root bridge. In the event of a network loop, data packets will pass through the port specified here.
- **Priority** Displays the priority number of the root bridge in the Spanning Tree. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used in determining the root bridge of a multi-bridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chances the bridge has of becoming the root bridge. A bridge priority ranges from 0 to 65535, with 0 being the highest priority.
- **Switch Priority** This is a read-only object that containing values from 0 to 65535. This value can be set in the Bridge Priority field and is the priority number of the bridge. The value is used in conjunction with the bridge MAC address to set the bridge ID, which in turn is used when determining the root bridge of a multi-bridged network. The root bridge is responsible for processing data packets when network loops occur. The smaller the number set, the higher the bridge priority is. The higher the bridge priority, the more chance the bridge has of becoming the root bridge. Zero is the highest priority.
- **Hello Time** Displays the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge.
- **Max Age** Read-only object indicates the maximum age of STP information learned from the network (on any port) before it is discarded.
- **Forward Delay** Displays the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

STP Parameter & Port Settings

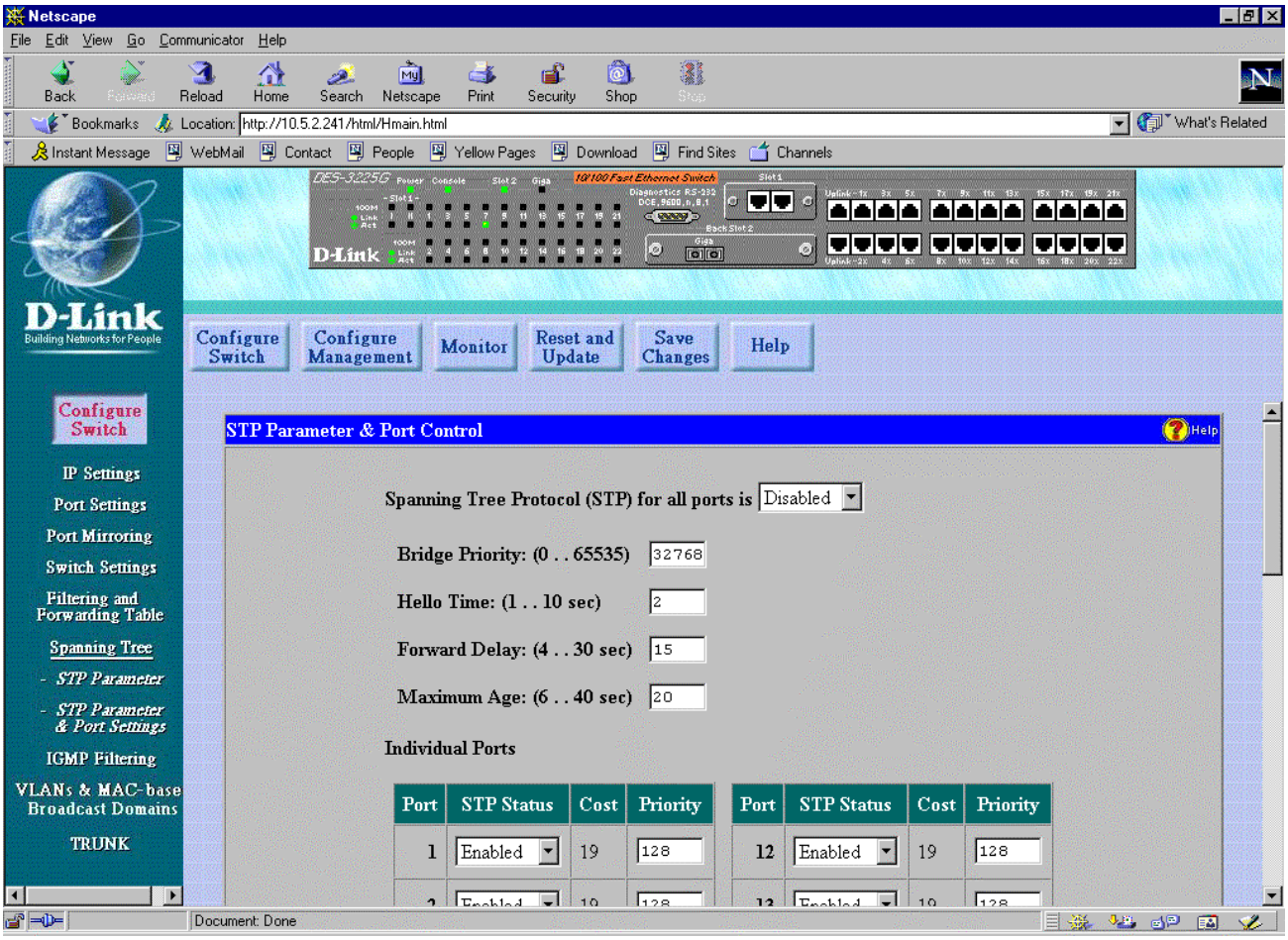

Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://10.5.2.241/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
Configure Switch
Configure Management
Monitor
Reset and Update
Save Changes
Help
Configure Switch
IP Settings
Port Settings
Port Mirroring
Switch Settings
Filtering and Forwarding Table
Spanning Tree
- STP Parameter
- STP Parameter & Port Settings
IGMP Filtering
VLANs & MAC-base Broadcast Domains
TRUNK
STP Parameter & Port Control
Help
Spanning Tree Protocol (STP) for all ports is Disabled
Bridge Priority: (0 . . 65535) 32768
Hello Time: (1 . . 10 sec) 2
Forward Delay: (4 . . 30 sec) 15
Maximum Age: (6 . . 40 sec) 20
Individual Ports
Port STP Status Cost Priority Port STP Status Cost Priority
1 Enabled 19 128 12 Enabled 19 128
Document: Done

Figure 7-14. STP Parameter & Port Control window

To configure Spanning Tree Protocol functions for the Switch or individual ports, enter the desired information in the fields on this window (see the descriptions below for assistance) and then click **Apply**.

The information on the window is described as follows:

- **Spanning Tree Protocol (STP) for all ports is** This option offers *Disabled* or *Enabled* to implement the Spanning Tree Protocol.
- **Bridge Priority: (0 .. 65535)/Priority** A Bridge Priority can be from 0 to 65535. Zero is equal to the highest Bridge Priority.
- **Hello Time: (1 . . 10 sec)** The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.
- **Forward Delay: (4 . . 30 sec)** The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.
- **Maximum Age: (6 . . 40 sec)** The Maximum Age can be from 6 to 40 seconds. At the end of the Maximum Age, if a BPDU has still not been received from the Root ridge, your Switch will start

sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

- **STP State** The Spanning Tree Protocol state for a selected port can either be *Enabled* or *Disabled*.
- **Cost** The Path Cost is a read-only parameter. The 100Mbps segment has an assigned Path Cost of 19, and each 10Mbps segment has an assigned Path Cost of 100.
- **Priority** Port Priority is a read-write object that can be set from 0 to 255. This is the priority number of the port. The lower the port priority, the more chance the bridge has of becoming the root port. Zero is the highest priority.

IGMP Filtering

IGMP Settings

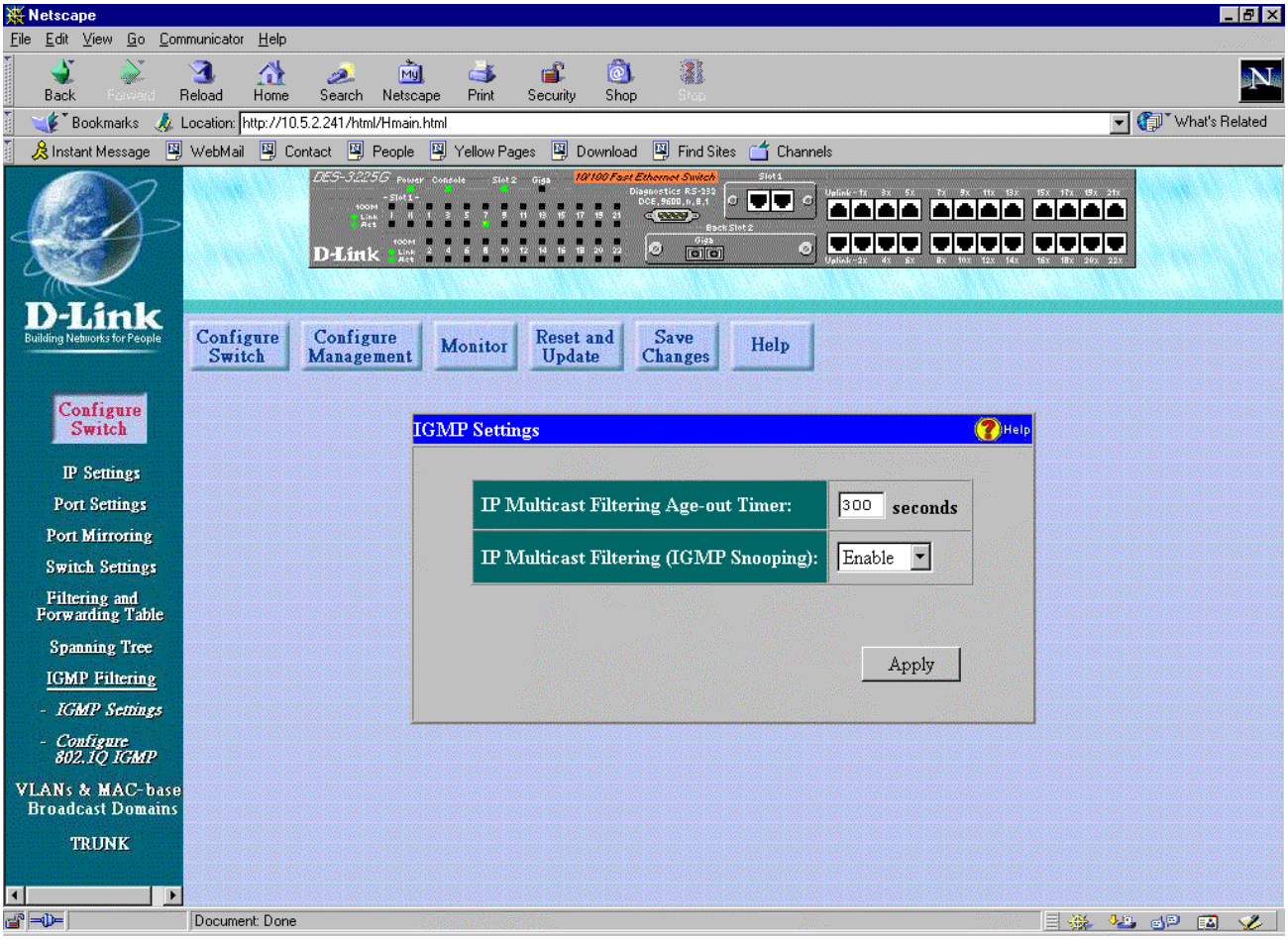


Figure 7-15. IGMP Settings window

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the switch.

To configure the IGMP, enter a value between 30 and 9999 seconds in the **IP Multicast Filtering Age-out Timer** field and then change the **IP Multicast Filtering (IGMP Snooping)** setting from *Disable* to *Enable*. Click the **Apply** button to let the changes take effect.

Items in the above window are described as follows:

- **IP Multicast Filtering Age-out Timer** When this timer elapses, the switch itself will try to become the IGMP host.
- **IP Multicast Filtering (IGMP Snooping)** This setting allows the switch to learn the IGMP spanning tree and intelligently forward packets (as opposed to broadcasting all packets). IGMP snooping is automatically enabled/disabled with this setting.

Configure 802.1Q IGMP

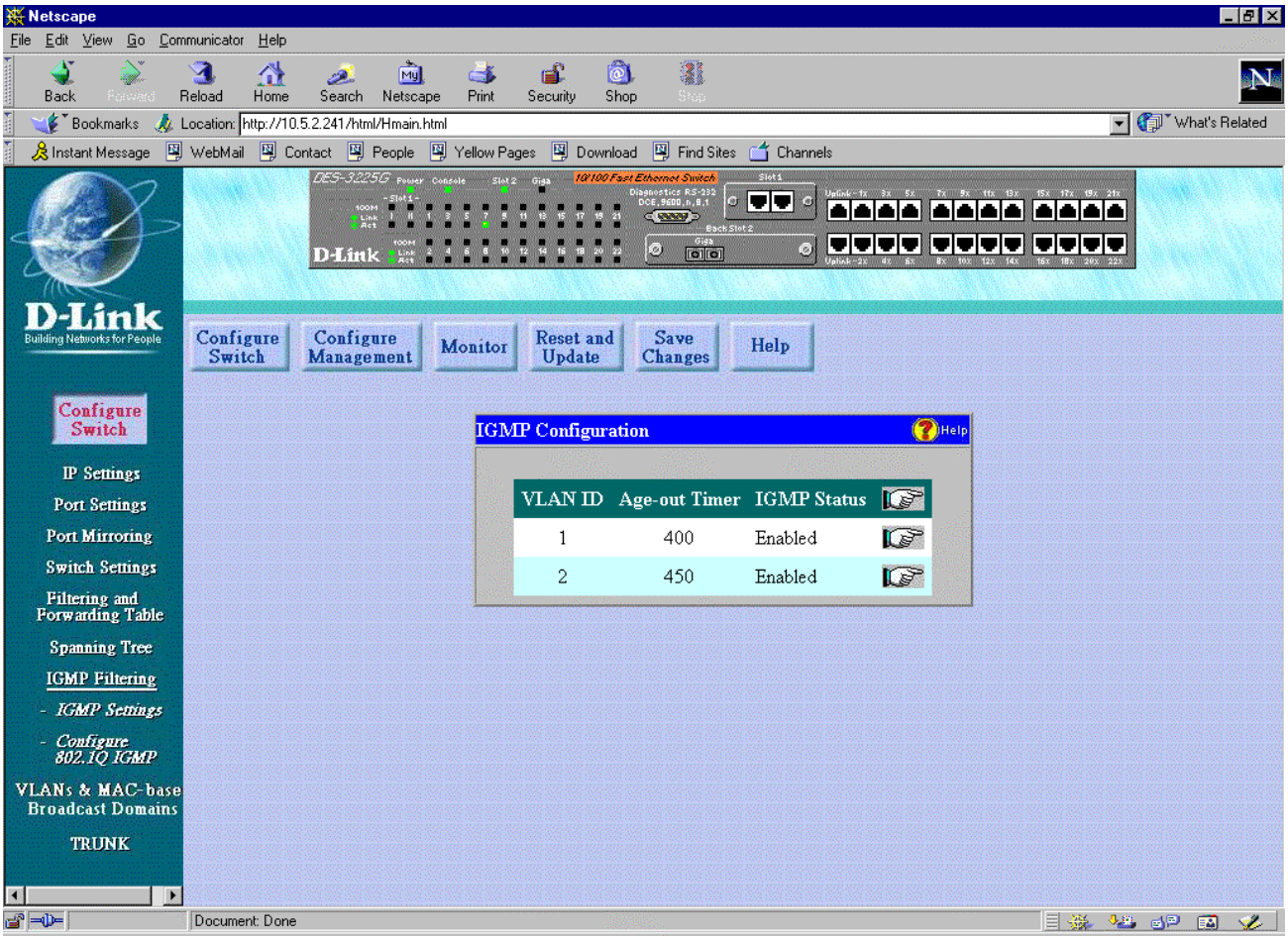


Figure 7-16. IGMP Configuration window

Click the icon on the far right to access the **Add/Delete IGMP Entry** window:

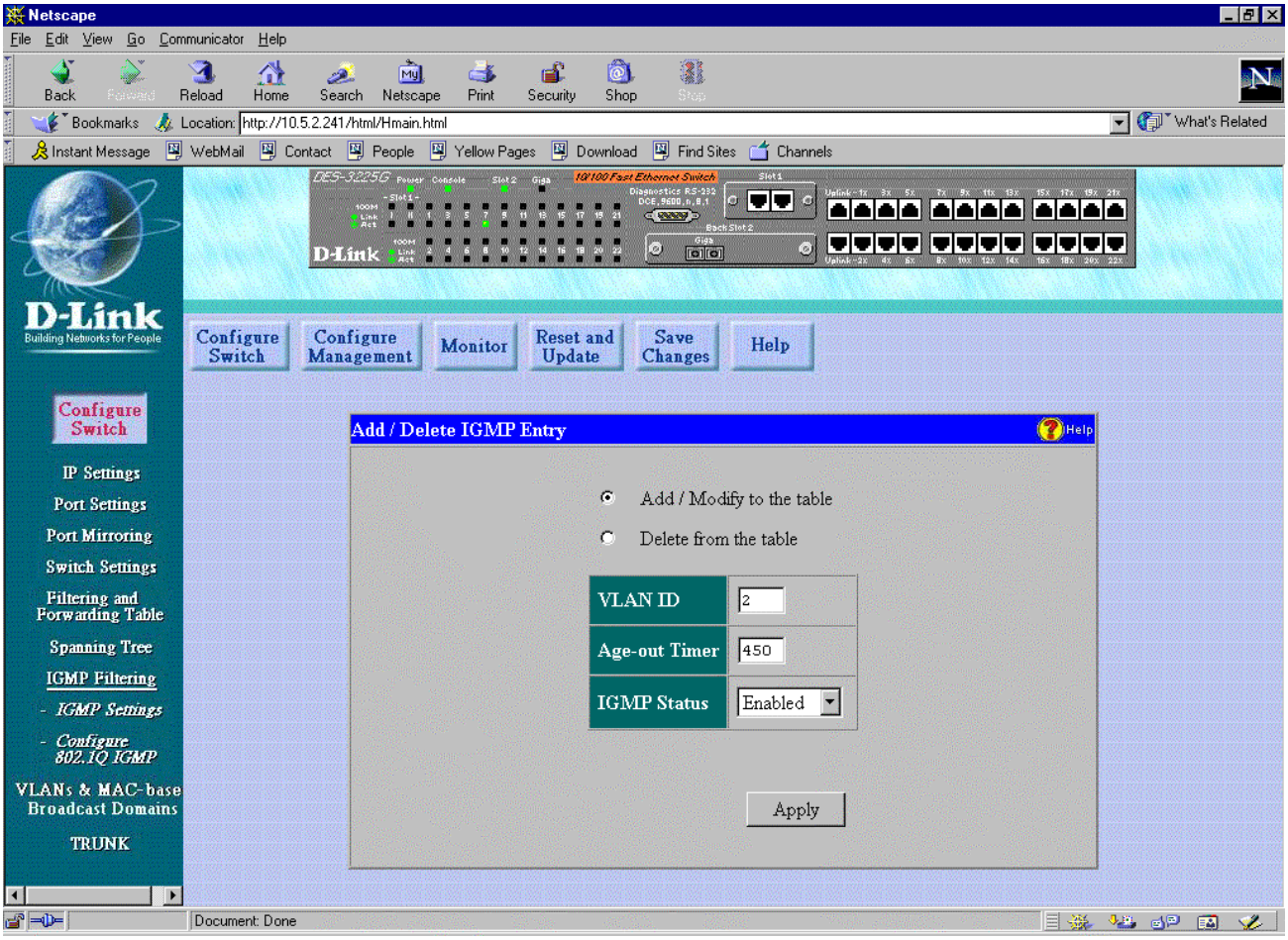


Figure 7-17. Add/Delete IGMP Entry window

To **Add/Modify to the table** or **Delete from the table**, check the desired option button, enter a value from 1 to 4094 in the **VLAN ID** field, enter a value between 30 and 9999 in the **Age-out Timer** field, enable or disable the **IGMP Status** control, and then click **Apply**.

The information above is described as follows:

- **Add/Modify to the table** Allows you to create or edit an entry for the table.
- **Delete from the table** Allows you to delete an IGMP entry from the table.
- **VLAN ID** This is the VLAN that will be defined on this screen. Note a VLAN ID is from 1 to 4094.
- **Age-out Timer** Specifies the time in seconds the switch will wait before trying to host IGMP on the VLAN.
- **IGMP Status** Enables/disables IGMP on this VLAN. Up to 12 VLANs can be enabled to handle IGMP packets at any one time.

VLANs & MAC-based Broadcast Domains

This section allows you to create Port-based VLANs, IEEE 802.1Q VLANs, and MAC-based Broadcast Domains. If unsure about this material, please consult Chapter 5, "Switch Management Concepts."

Configure VLANs & MAC-based Domains

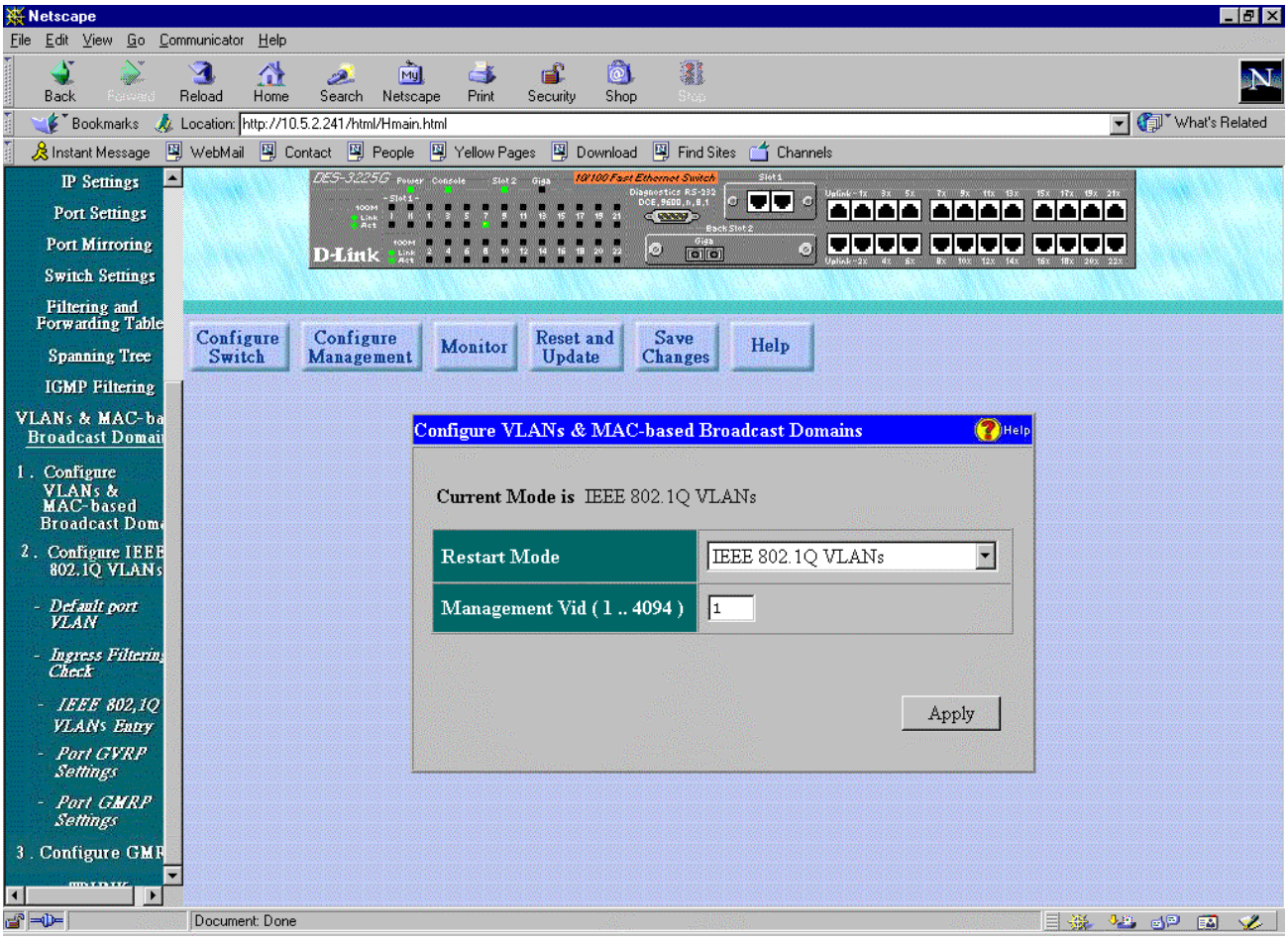


Figure 7-18. Configure VLANs & MAC-based Broadcast Domains window

To configure VLANs and MAC-based Broadcast Domains, select *MAC-based Broadcast Domains, IEEE 802.1Q VLANs*, or *Port-based VLAN* under **Restart Mode**--otherwise, leave the setting at *None*. Then specify the VLAN ID number in the **Management Vid (1.. 4094)** field and click **Apply**.

The information above is described as follows:

- **Restart Mode** Choose from four settings for this mode: *MAC-based Broadcast Domains*, *Port-based VLAN, IEEE 802.1Q VLANs,* or *None*.

- **Management Vid (1..4094)** When *IEEE 802.1Q VLANs* or *Port-based VLAN* are enabled, this is the VLAN that will be used for management packets. Make sure the switch port that the management station is connected to has this PVID number and is a member of this 802.1Q VLAN (VID). This should be the first VLAN you create, otherwise, you may not be able to communicate with the Switch except through the console port.

Configure IEEE 802.1Q VLANs

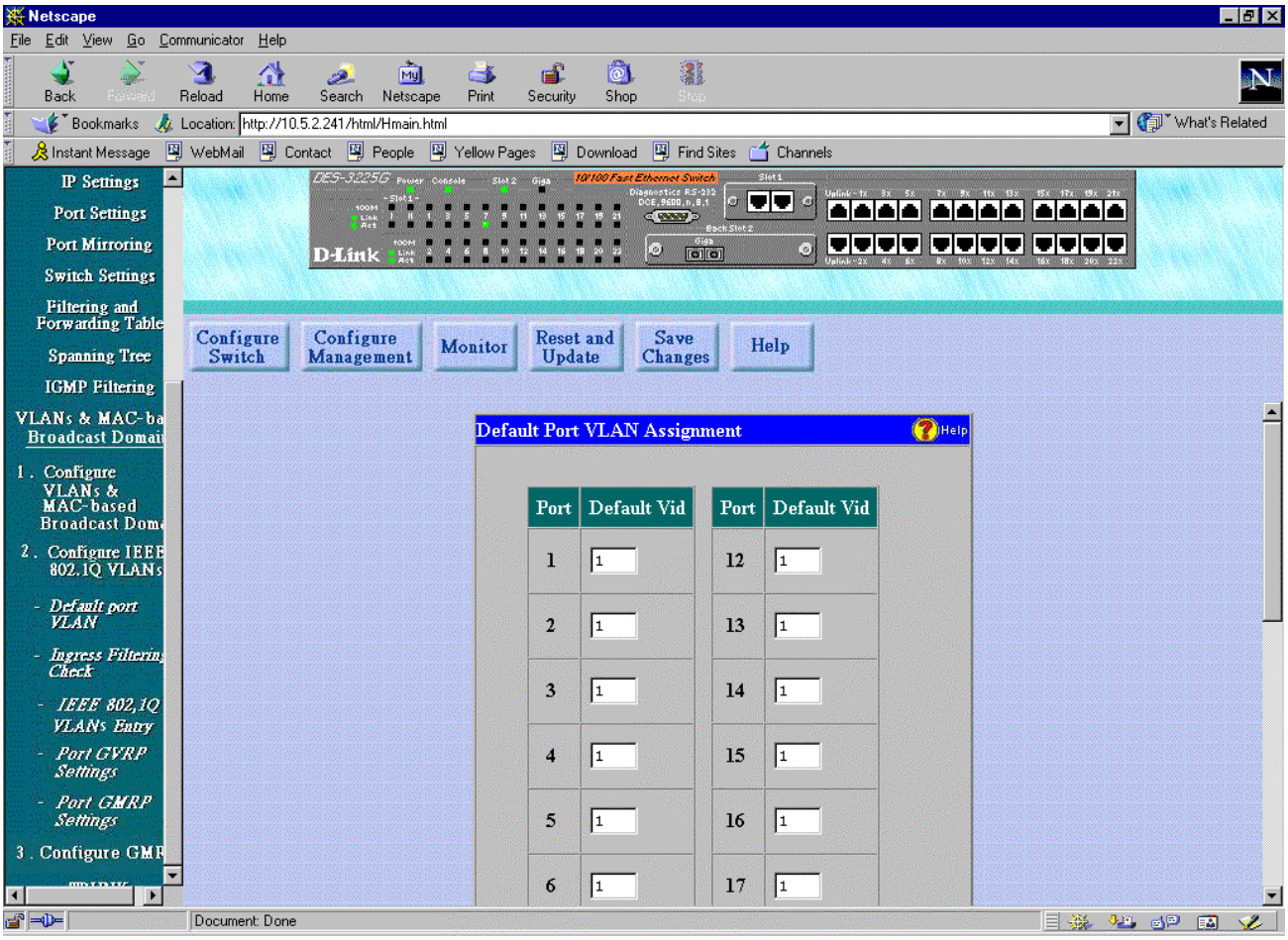


Figure 7-19. Default Port VLAN Assignment window

Use this window to assign a Port VLAN ID (PVID) number for each port. Click **Apply** to let the settings take effect. Please note that this function only applies to *IEEE 802.1Q VLANs* mode.

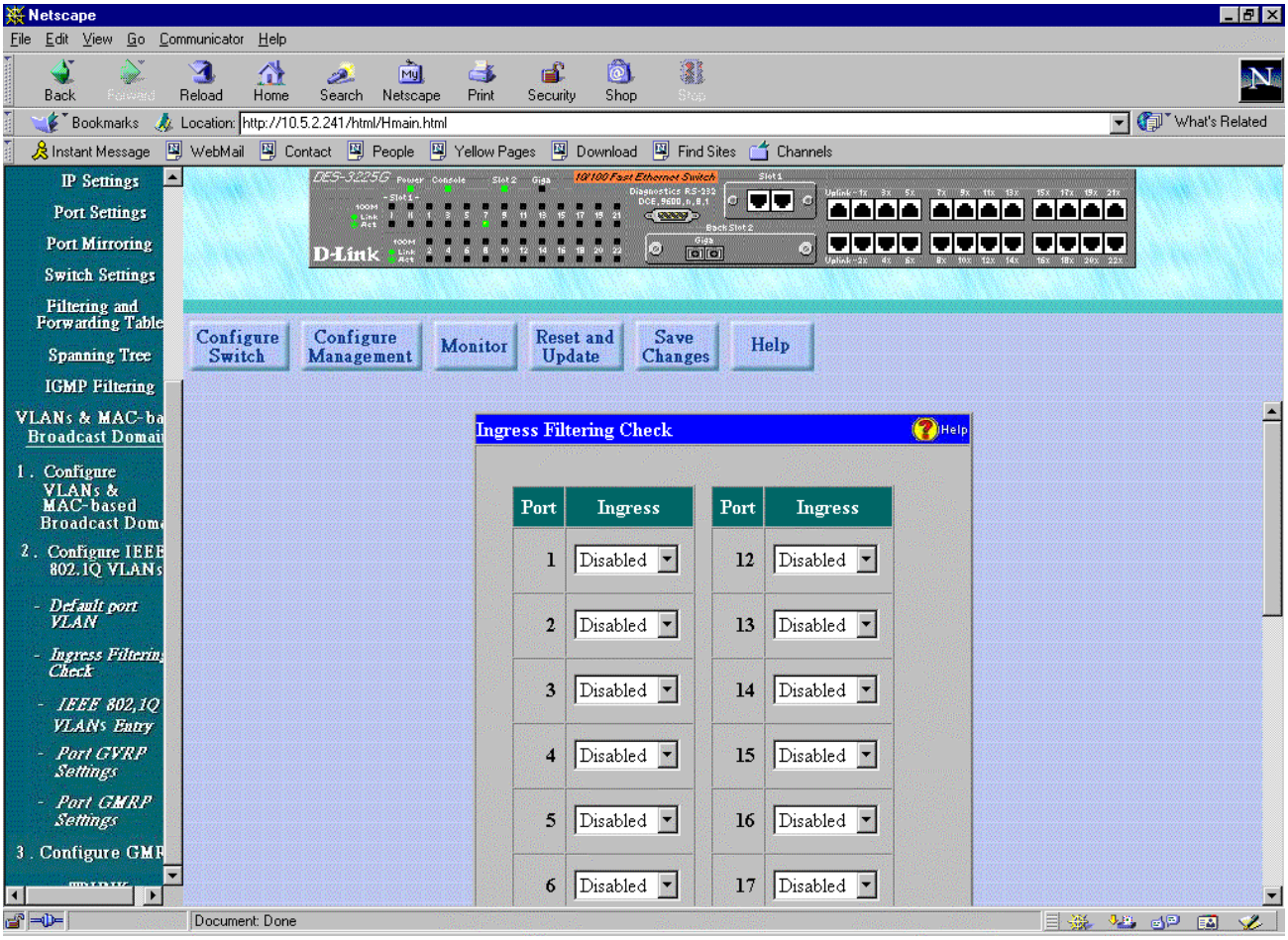


Figure 7-20. Ingress Filtering Check window

Use this window to enable or disable the ingress filtering check for each desired port. Ingress filtering means that a receiving port will check to see if it is a member of the VLAN ID in the packet before forwarding the packet. Click **Apply** to let the settings take effect. Please note that this function only applies to *IEEE 802.1Q VLANs* mode.

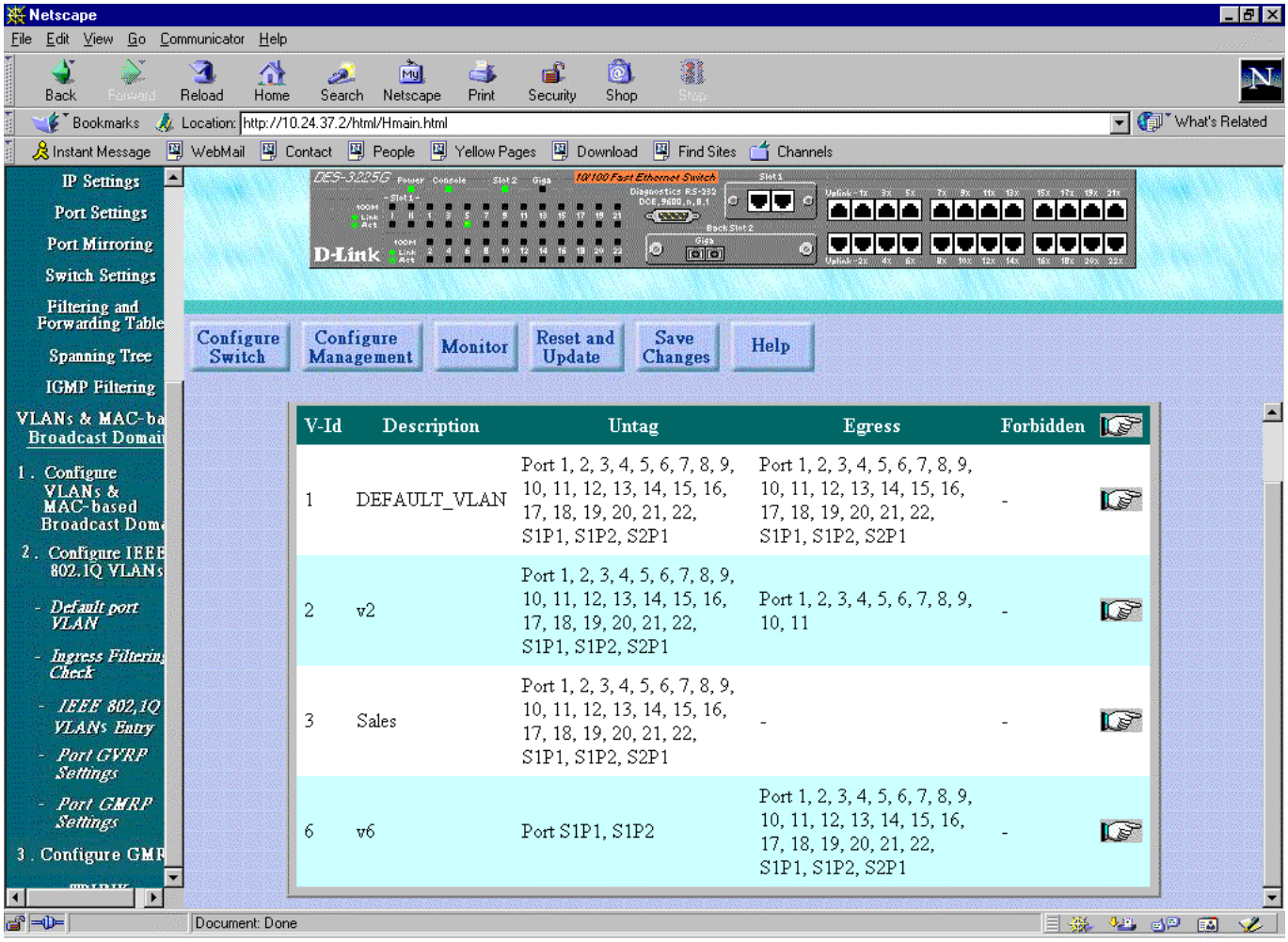

Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://10.24.37.2/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
IP Settings
Port Settings
Port Mirroring
Switch Settings
Filtering and Forwarding Table
Spanning Tree
IGMP Filtering
VLANs & MAC-ba
Broadcast Domai
1. Configure VLANs & MAC-based Broadcast Dom
2. Configure IEEE 802.1Q VLANs
- Default port VLAN
- Ingress Filterin Check
- IEEE 802.1Q VLANs Entry
- Port GVRP Settings
- Port GMRP Settings
3. Configure GMR
Configure Switch
Configure Management
Monitor
Reset and Update
Save Changes
Help
V-Id
Description
Untag
Egress
Forbidden
1 DEFAULT_VLAN Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, S1P1, S1P2, S2P1 Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, S1P1, S1P2, S2P1 -
2 v2 Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, S1P1, S1P2, S2P1 Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 -
3 Sales Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, S1P1, S1P2, S2P1 - -
6 v6 Port S1P1, S1P2 Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, S1P1, S1P2, S2P1 -
Document: Done

Figure 7-21. Configure IEEE 802.1Q VLANs window

Please note that this function only applies to *IEEE 802.1Q VLANs* mode.

Click the pointer icon on the right side to access the **Configure IEEE 802.1Q VLANs Entry** window:

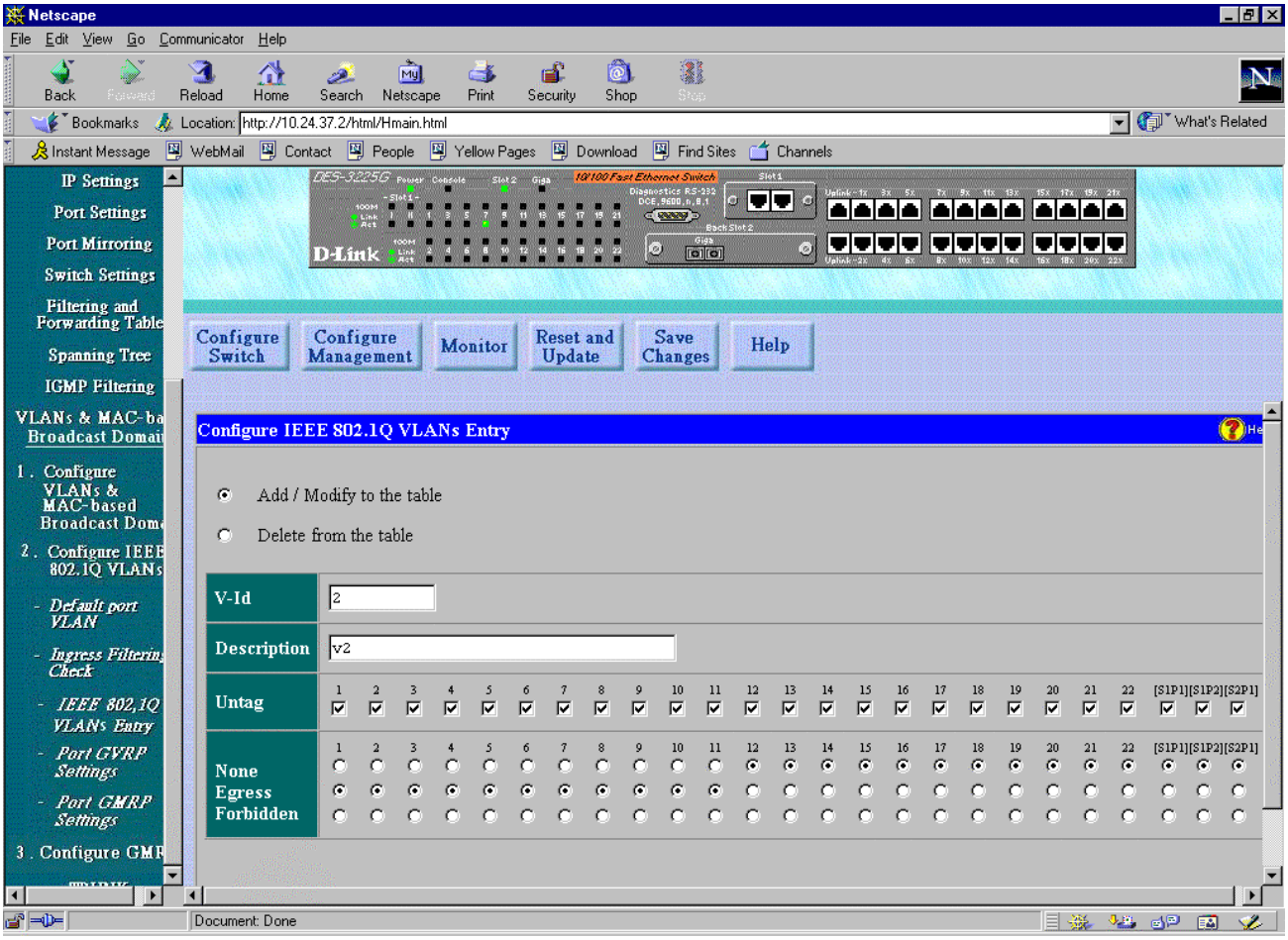


Figure 7-22. Configure IEEE 802.1Q VLANs Entry window

To configure an 802.1Q VLAN entry, check the desired option in the first two lines of the window above and enter a V-Id number and Description. Next, either check the Untag option, or leave it unchecked for each member port you wish to be a *Tagging* port. In the bottom three lines, None should be checked if you don't want a port to belong to the VLAN. Otherwise, check Egress to statically set a port to belong to a VLAN or check Forbidden if you wish to forbid the port from dynamically belonging to the VLAN. Click **Apply** to let the changes take effect. Please note that this function only applies to *IEEE 802.1Q VLANs* mode.

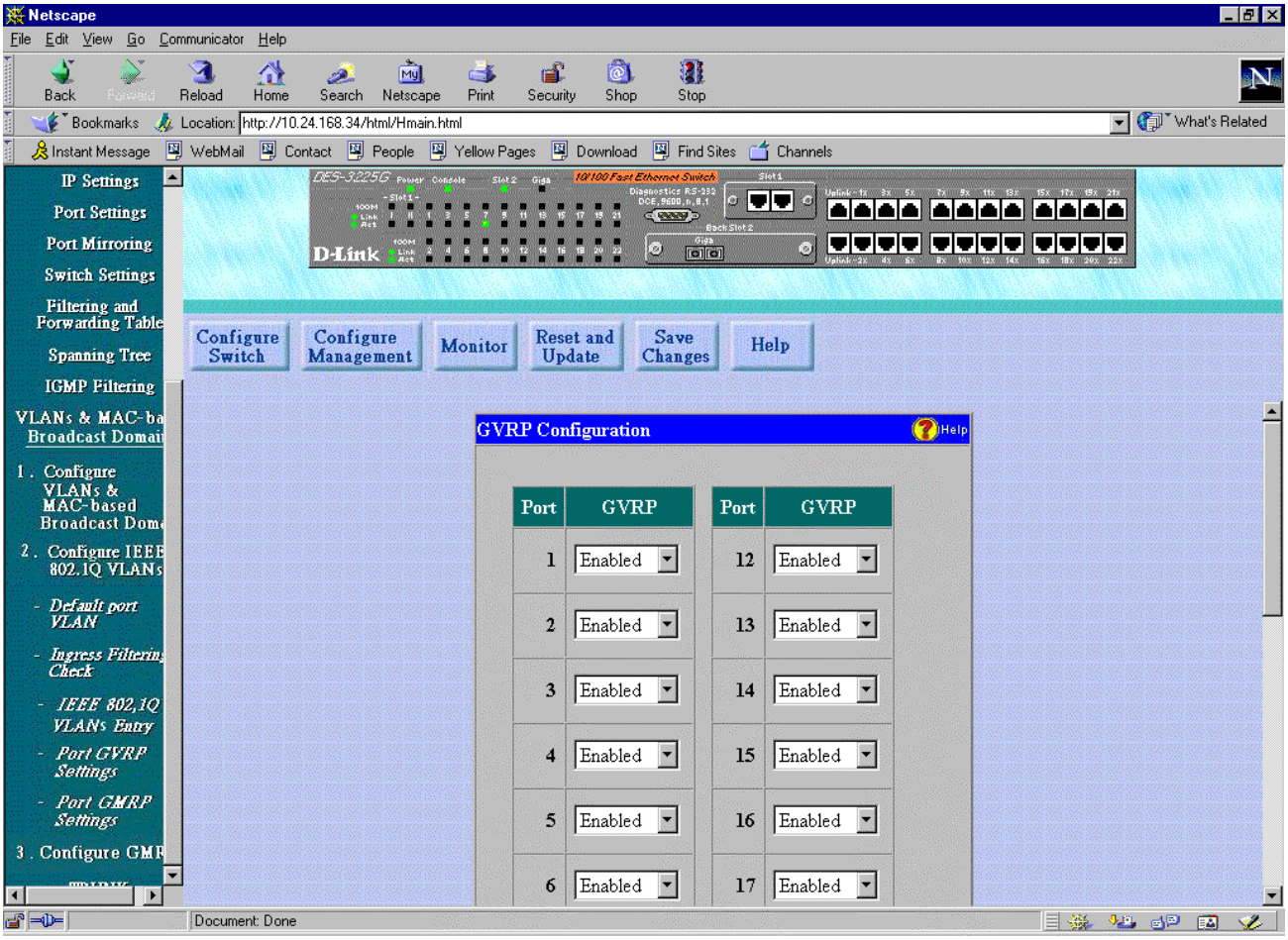


Figure 7-23. GVRP Configuration window

This window allows you to enable or disable GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol, on individual ports.

GVRP updates dynamic VLAN registration entries and communicates the new VLAN information across the network. This allows, among other things, for stations to physically move to other switch ports and keep their same VLAN settings, without having to reconfigure VLAN settings on the Switch.

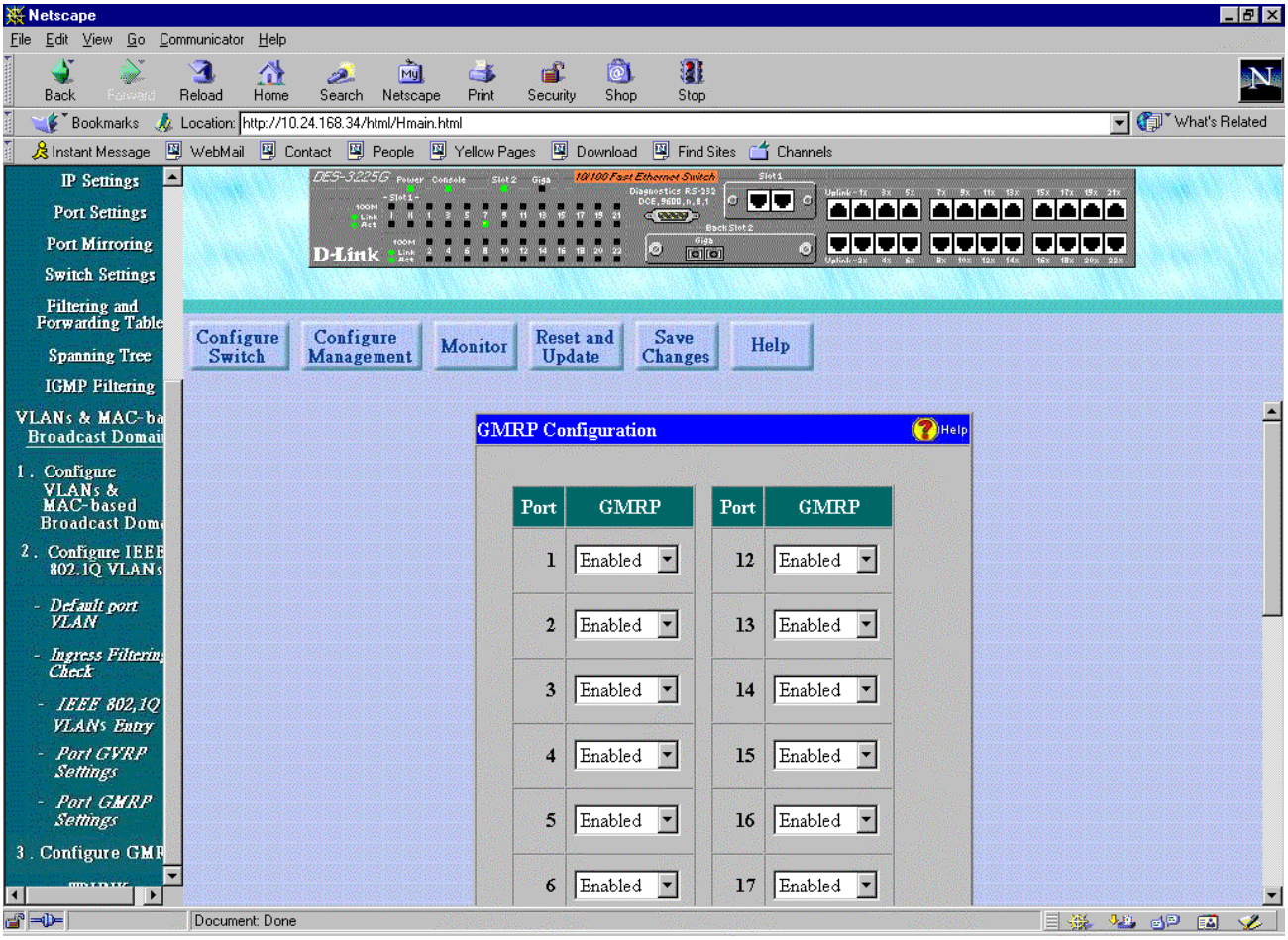


Figure 7-24. GMRP Configuration window

This window allows you to either enable or disable GMRP on a specific port. Press APPLY to let your changes take effect.

Trunk

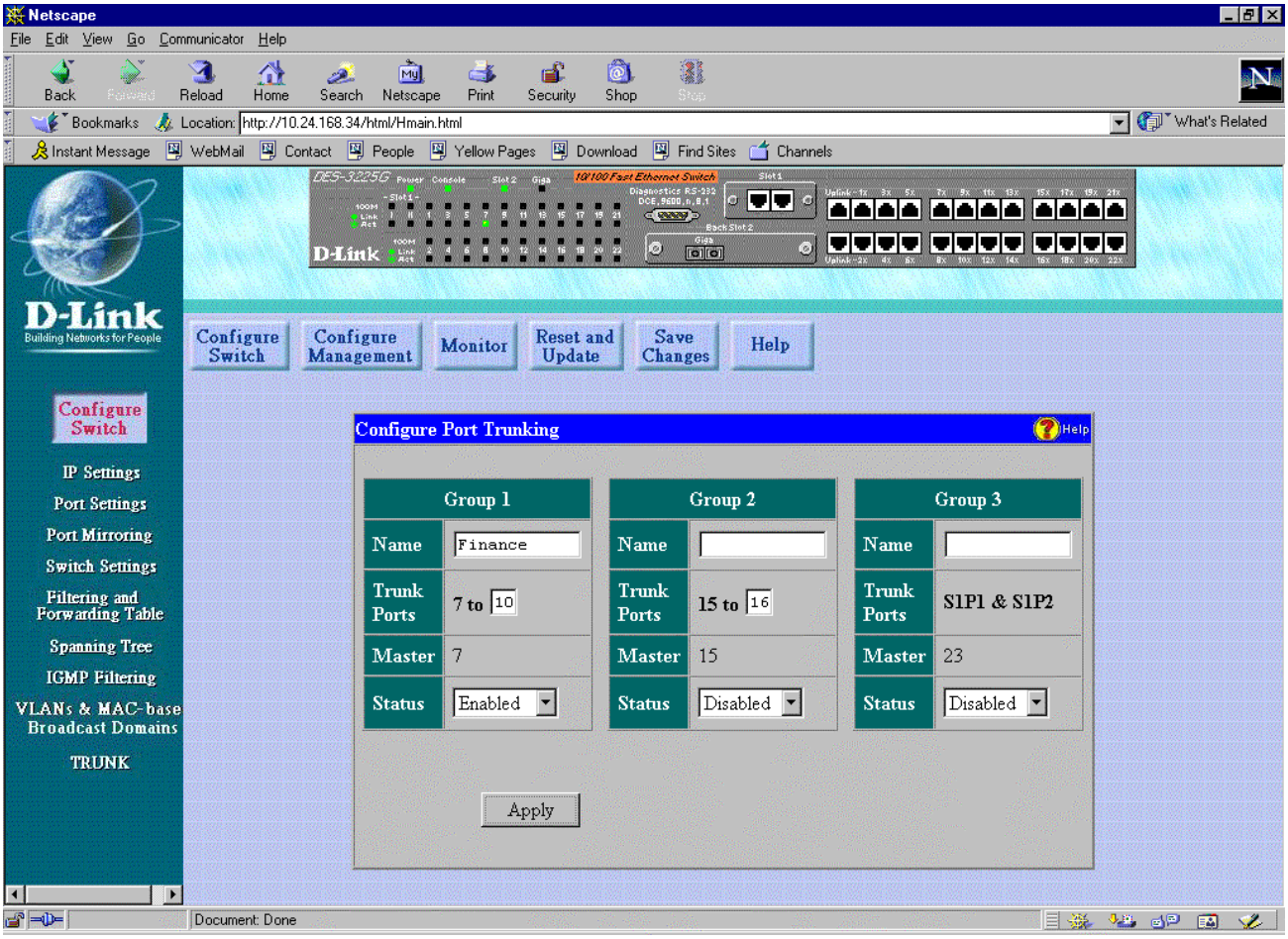


Figure 7-25. Configure Port Trunking window

The Switch supports up to 3 trunk groups. Trunks are groups of ports that are banded together to form a single, logical, high-bandwidth data pipe.

Items in the above window are defined as follows:

- **Name** The user-assigned name of the trunk group.
- **Trunk Ports** The continuous number of ports that will be members of the trunk group.
- **Master** The Master port for the trunk group. All configuration settings changes made to the master port will automatically be made to the other ports in the trunk.
- **Status** Enables or disables the trunk group.

Configure Management

This second category includes: **Traps and Community Strings**, **User Accounts**, and **Console Port Settings**.

Traps and Community Strings

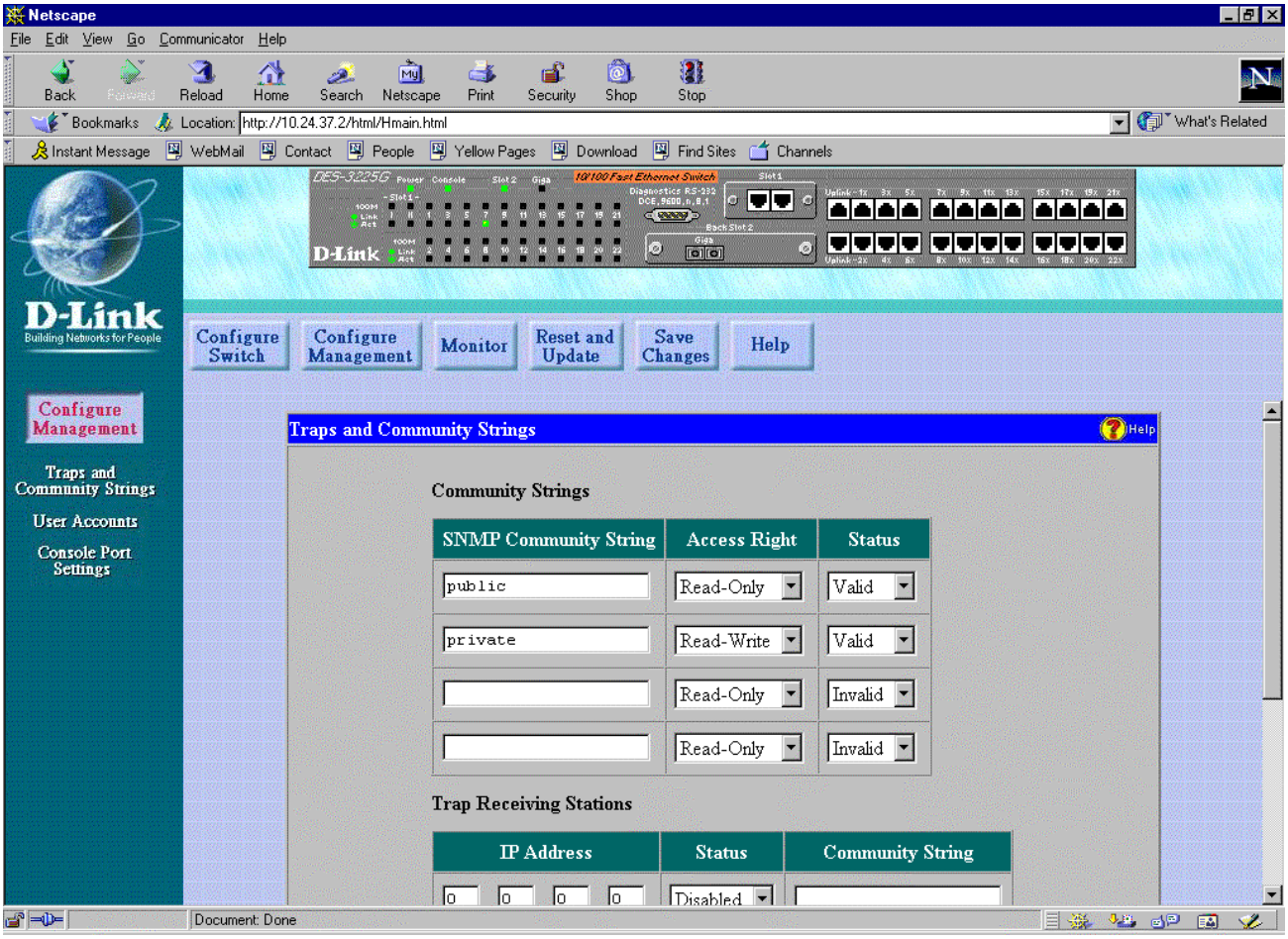


Figure 7-26. Traps and Community Strings window

To use the functions on this window, enter the appropriate SNMP information in the Community Strings and Trap Receiving Stations sections--you may enter up to four entries in each section. A trap receiving station is a device that constantly runs a network management application to receive and store traps. Then click **Apply** to put the settings into effect.

The Community Strings information is described as follows:

- **SNMP Community String** A user-defined SNMP community name.
- **Access Right** The permitted access of *Read-Only* or *Read-Write* using the SNMP community name.
- **Status** Option to set the current community string to *Valid* or *Invalid*.

The Trap Receiving Stations information is described as follows:

- **IP Address** The IP address of the trap receiving station.
- **Status** Option to set the trap receiving station to *Enabled* or *Disabled*.
- **Community String** A user-defined SNMP community name.

User Accounts

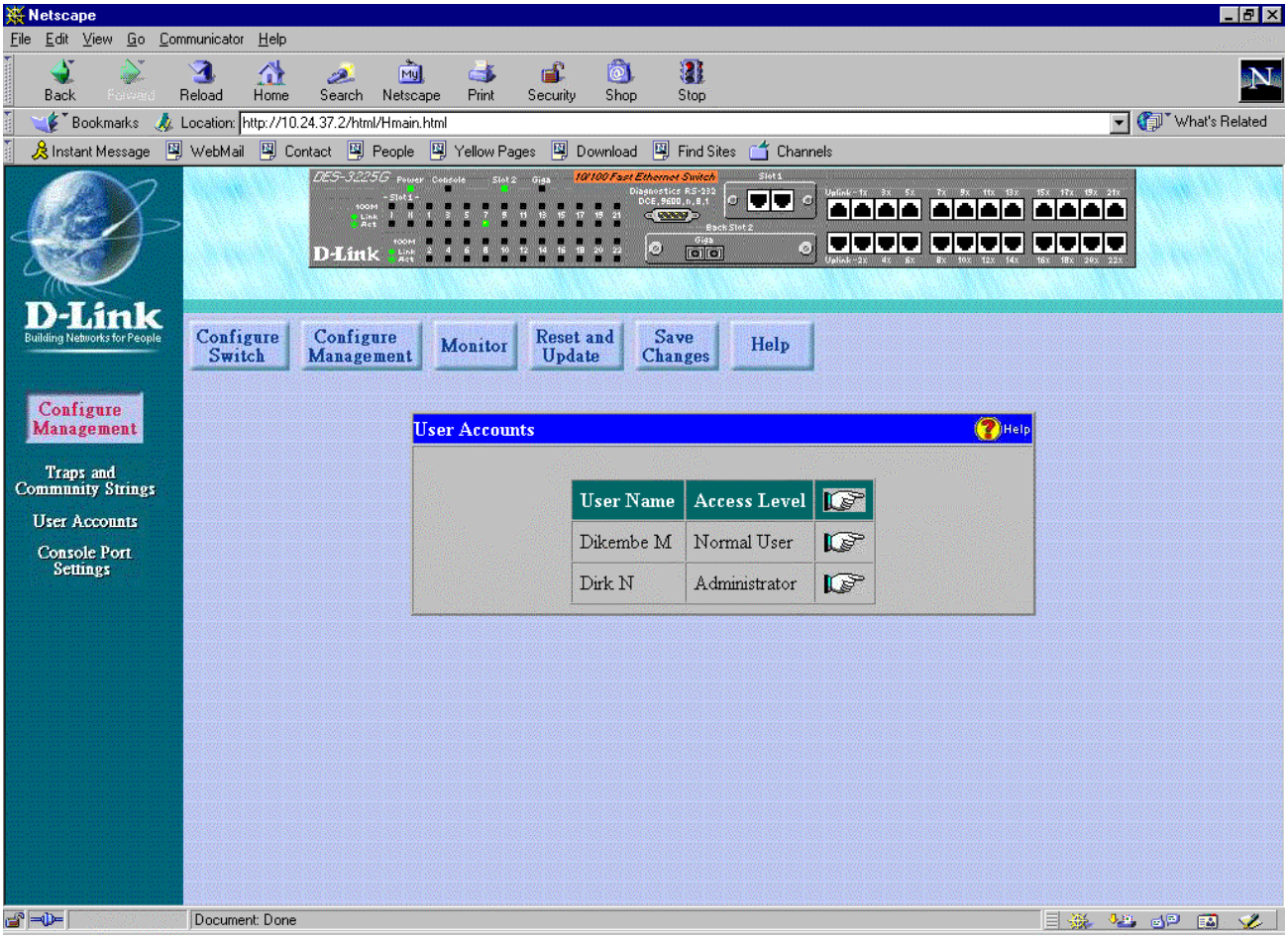


Figure 7-27. first User Accounts window

Click the pointer icon on the right side to access the main **User Accounts** window:

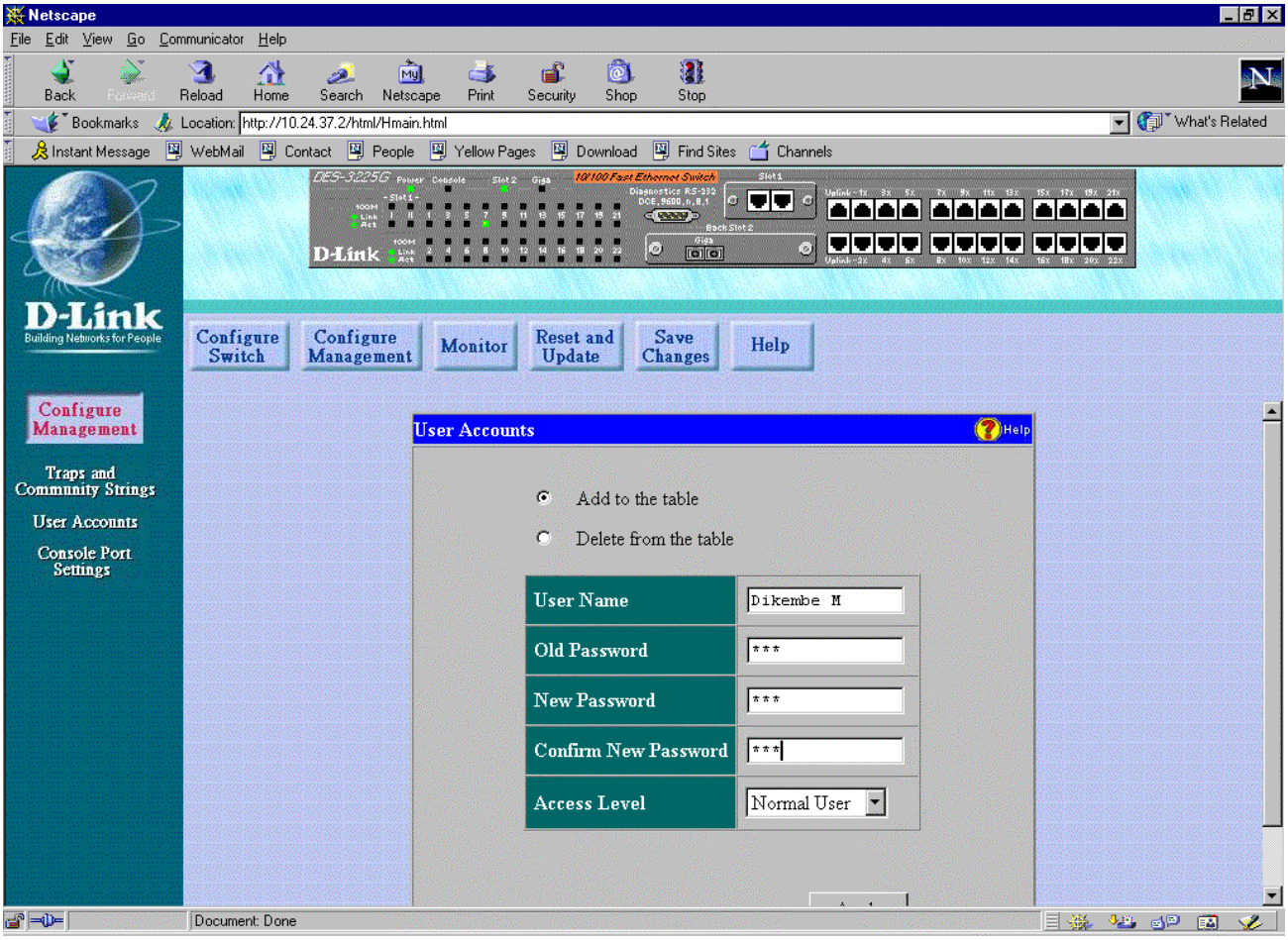


Figure 7-28. second User Accounts window

To add or delete a User Account, fill in the appropriate information in the User Name, Old Password, New Password, and Confirm New Password fields. Then select the desired access, *Normal User* or *Administrator* in the Access Level control and click **Apply**.

Console Port Settings

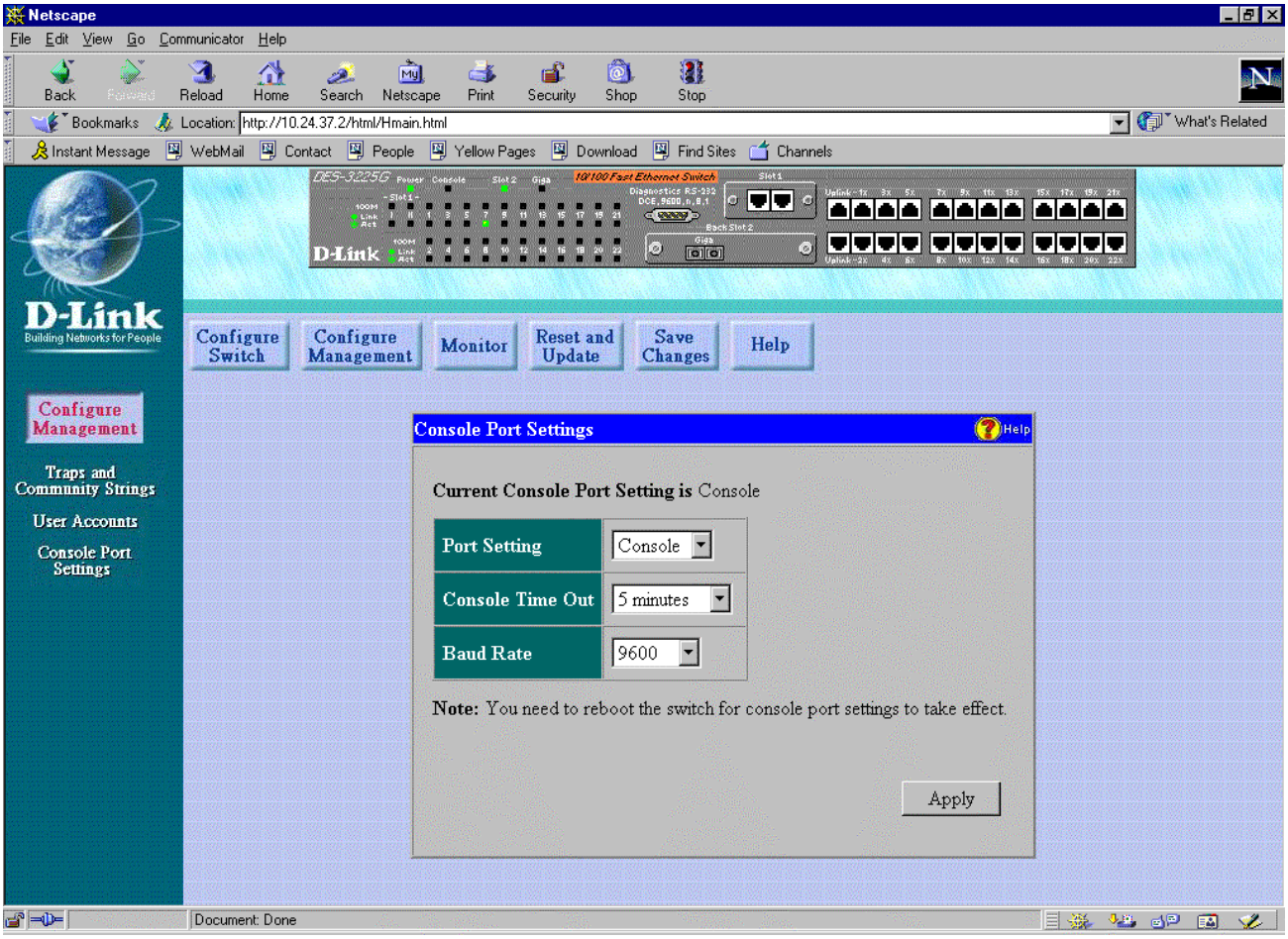


Figure 7-29. Console Port Settings window

This window allows you to select the protocol for communicating through the console port, *Console* or *SLIP,* in the **Port Setting** field. Use SLIP for out-of-band management. You can also choose the refresh rate in the **Console Time Out** field (*2 minutes*, *5 minutes*, *10 minutes*, *15 minutes* or *Never*). If SLIP is being used, you may also set the **Baud Rate** in the last field. Click **Apply** and then reboot the Switch for console port settings to take effect.

The default serial port settings are:

Baud Rate=9600

Data Bits=8

Flow Control=X on/X off

Parity=None

Stop Bits=1

The information is described as follows:

- **Port Settings** The options for the current console port setting are *Console* or *SLIP*.
- **Console Time Out** Choose *Never*, *2 minutes*, *5 minutes, 10 minutes*, or *15 minutes* for the desired refresh setting.

- **Baud Rate** Determines the serial port bit rate that will be used the next time the Switch is restarted. Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are 2400, 9600, 19,200 and 38,400 bits per second. The default setting in this Switch version is 9600.

Monitor

This third category includes: **Switch Overview**, **Port Statistics** (**Traffic**, **Errors**, **Packet Analysis**, and **Utilization**), **Browse Address Table**, **Browse IGMP Status**, **Browse GVRP Status**, **Browse GMRP Status**, and **Switch History**.

Switch Overview

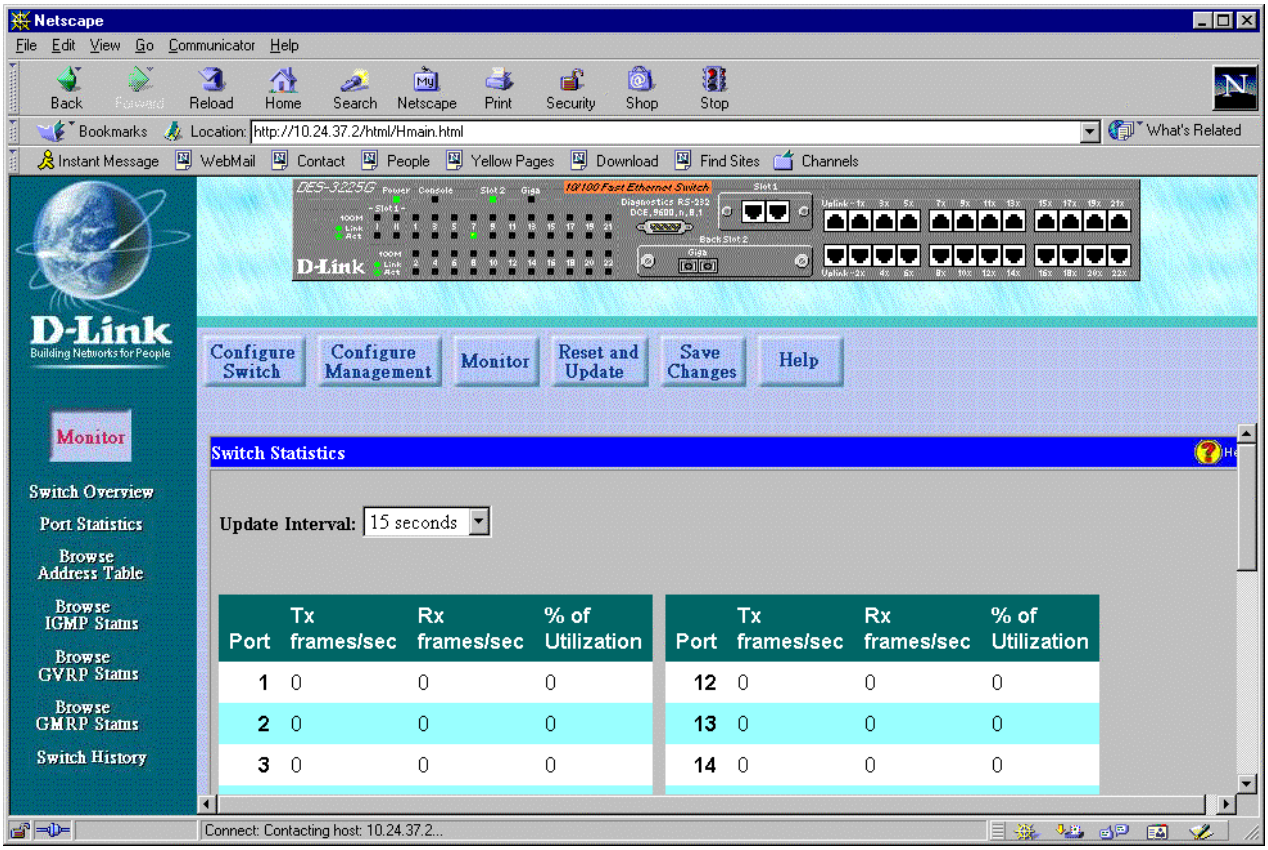

Netscape
File Edit View Go Communicator Help
Back Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://10.24.37.2/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
Configure Switch
Configure Management
Monitor
Reset and Update
Save Changes
Help
Monitor
Switch Overview
Port Statistics
Browse Address Table
Browse IGMP Stats
Browse GVRP Stats
Browse GMRP Stats
Switch History
Switch Statistics
Update Interval: 15 seconds
Port Tx frames/sec Rx frames/sec % of Utilization Port Tx frames/sec Rx frames/sec % of Utilization
1 0 0 0 12 0 0 0
2 0 0 0 13 0 0 0
3 0 0 0 14 0 0 0
Connect: Contacting host: 10.24.37.2...

Figure 7-30. Switch Statistics window

The information is described as follows:

- **Update Interval** Choose the desired setting: *2 seconds*, *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.
- **Port** The selected port to be monitored.
- **TX frames/sec** Counts the total number of frames transmitted from a selected port per second since the Switch was last rebooted.
- **RX frames/sec** Counts all valid frames received on the port per second since the Switch was last rebooted.

- **% of Utilization** This shows the percentage of available bandwidth each port is using over the amount of time specified by the update interval. For example, when a 10 Mbps port is relaying packets at 5 Mbps, the utilization is 50%.

Port Statistics

The port statistics shown by default are those for the port you last configured. Once in the Port Statistics windows, you can click any port on the switch graphic to show statistics for that port. Click the **Reset Counter** button at the bottom of the window to clear the counters.

Traffic

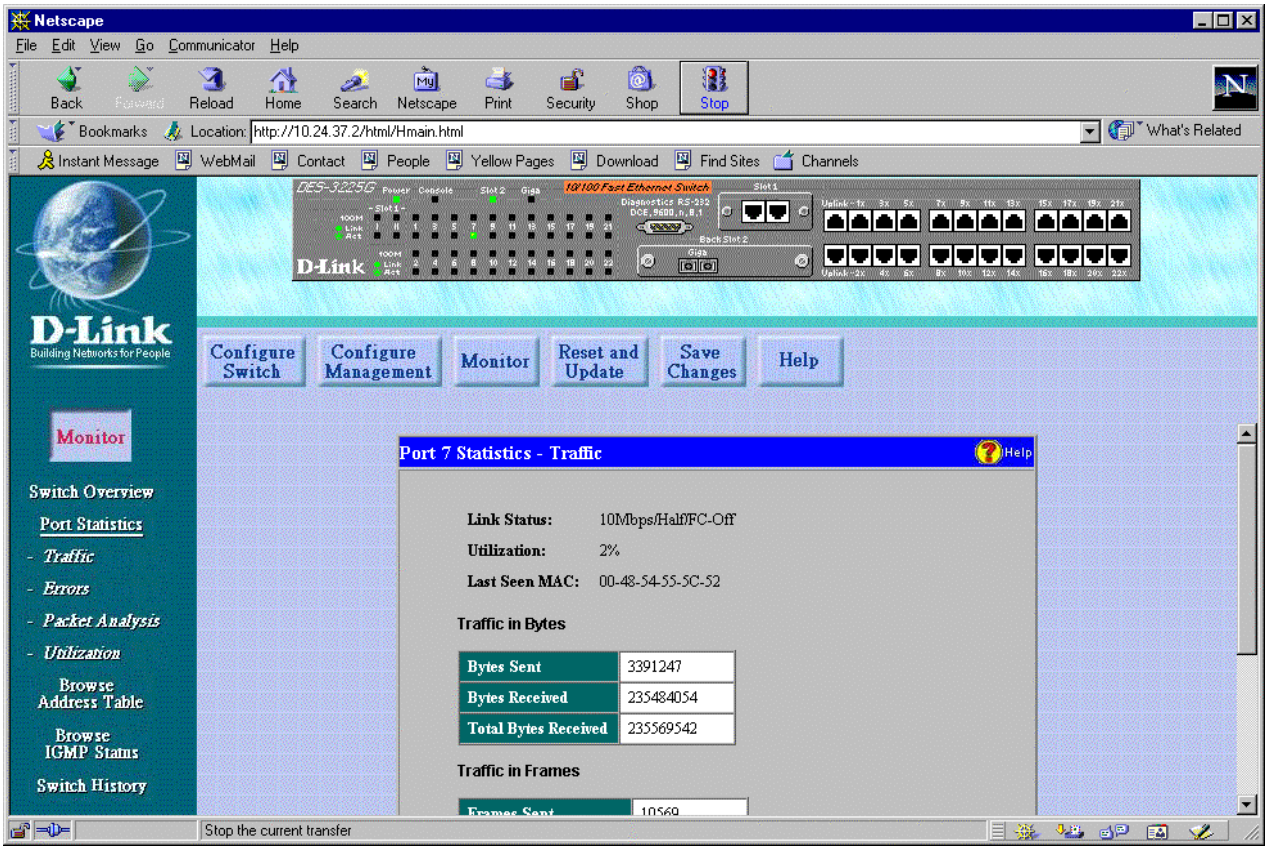


Figure 7-31. Port Statistics - Traffic window

The information is described as follows:

- **Link Status** Indicates whether the port is online and working (*On*) or not (*Off*).
- **Utilization** Current utilization for the port, as a percentage of total available bandwidth.
- **Last Screen MAC** The MAC address of the most recent screen.

Traffic in Bytes:

- **Bytes Sent** Counts the number of bytes successfully sent from the port.
- **Bytes Received** Counts the total number of bytes (octets) included in valid (readable) frames.
- **Total Bytes Received** Counts the total number of bytes received on the port, whether in valid or invalid frames.

Traffic in Frames:

- **Frames Sent** Counts the total number of frames transmitted from the port.
- **Frames Received** Counts all valid frames received on the port.
- **Total Frames Received** Counts the number of frames received on the port, whether they were valid or not.

Errors

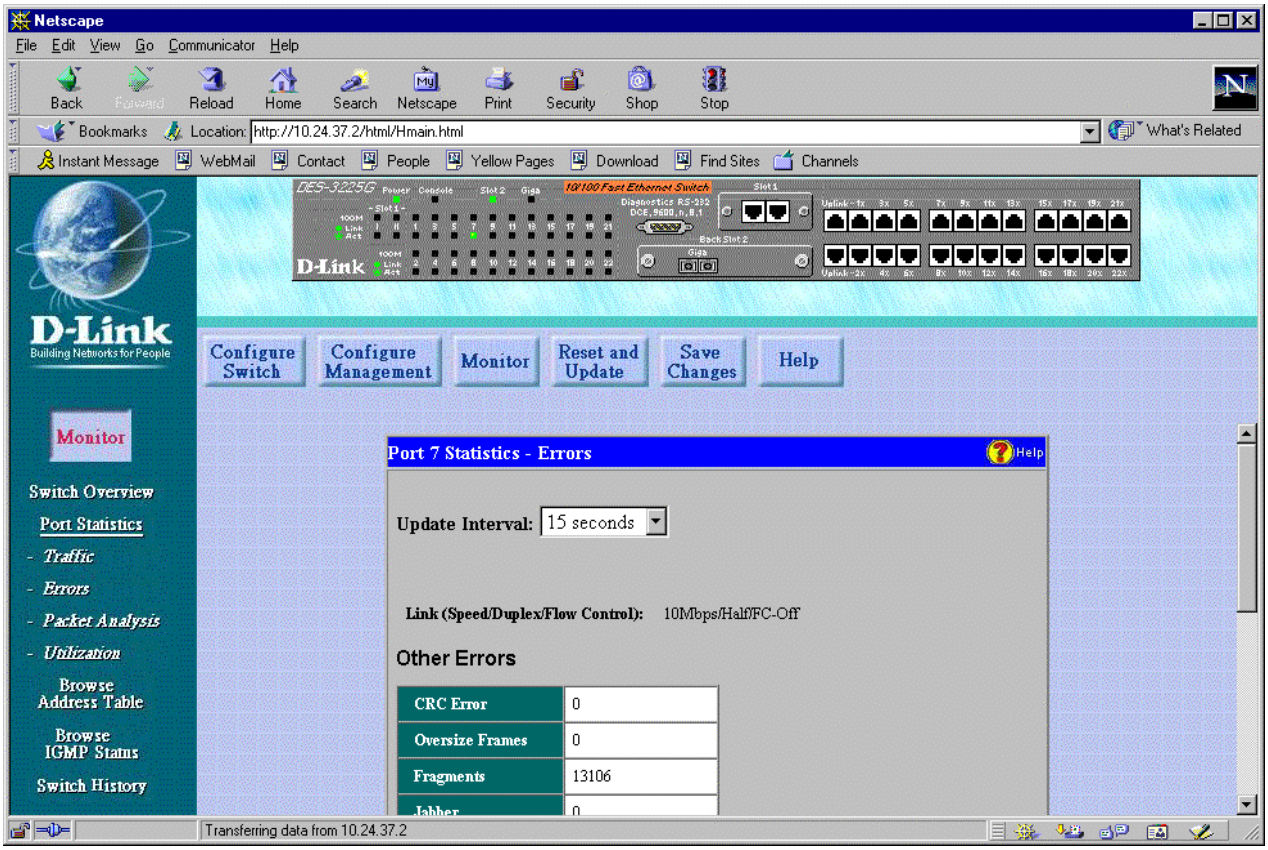


Figure 7-32. Port Statistics - Errors window

The information is described as follows:

- **Update Interval** Choose the desired setting: *2 seconds*, *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.
- **Link (Speed/Duplex/Flow Control)** Indicates the current link status.

Other errors:

- **CRC Error** Counts otherwise valid frames that did not end on a byte (octet) boundary.
- **Oversize Frames** Counts packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
- **Fragments** The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

- **Jabber** The number of frames with length more than 1518 bytes and with CRC error or misalignment (bad framing).
- **Late Collision** Counts collisions that occur at or after the 64th byte (octet) in the frame. This may indicate that delays on your Ethernet are too long, and you have either exceeded the repeater count or cable length specified in the Ethernet standard.
- **MAC Received Error** Counts data errors detectable as 10BASE-TX "symbol errors," bit patterns with illegal encodings. This may indicate noise on the line.
- **Dropped Frames** The number of frames which are dropped by this port since the last Switch reboot.
- **Undersize Frames** The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
- **Total Errors** The sum of the CRC Error, Oversize Frames, Fragments, Jabber, Late Collision, MAC Received Error, Dropped Frames, and Undersize Frames counters.
- **Collisions** The best estimate of the total number of collisions on this Ethernet segment.

Packet Analysis

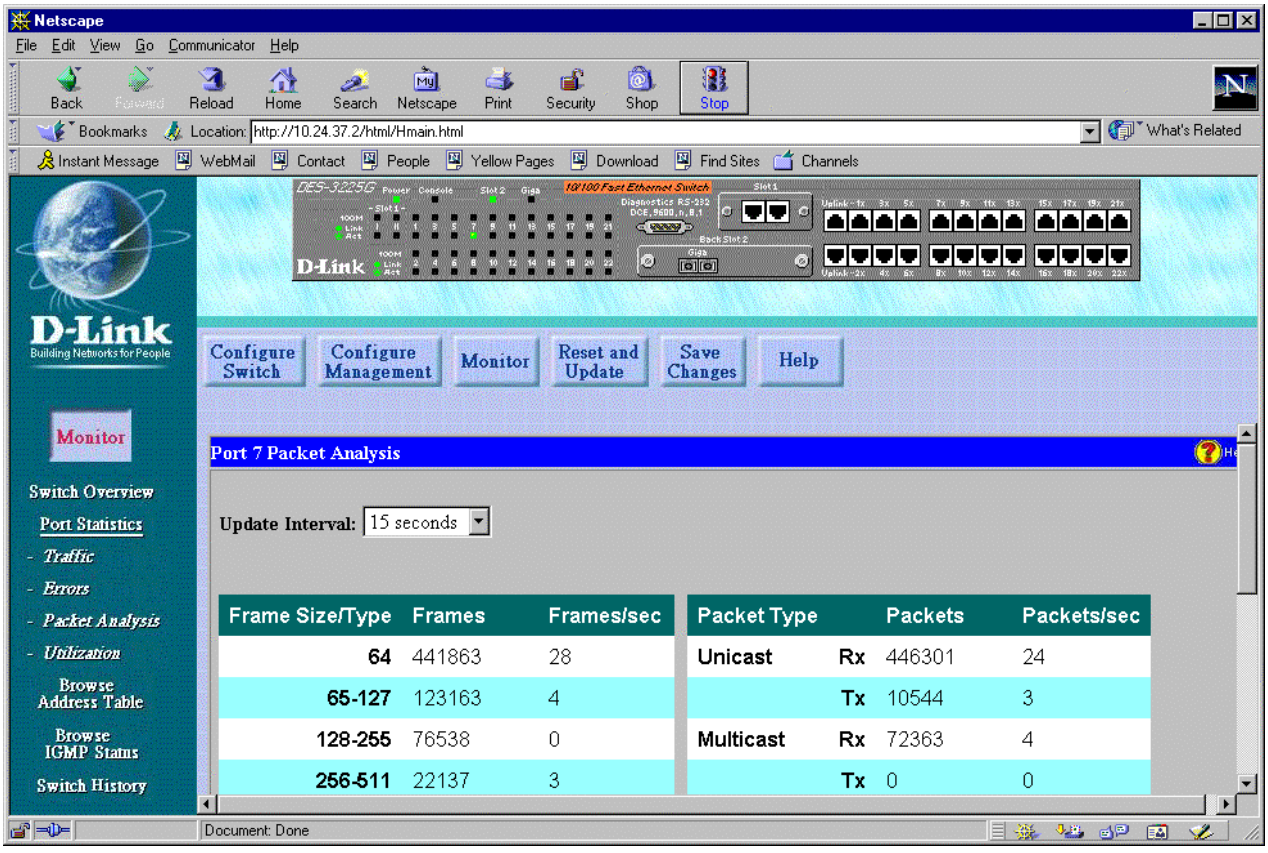


Figure 7-33. Port Packet Analysis window

The information is described as follows:

- **Update Interval** Choose the desired setting: *2 seconds*, *5 seconds*, *15 seconds*, *30 seconds*, *60 seconds* or *Suspend*.

- **64** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
- **65-127** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
- **128–255** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
- **256-511** The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
- **512-1023** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
- **1024-1518** The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
- **Rx (good)** The number of good frames received. This also includes local and dropped packets.
- **Tx (good)** The number of good frames sent from the respective port.
- **Total Rx** The number of frames received, good and bad.
- **Tx Bytes** The number of good bytes sent from the respective port.
- **Rx Bytes** The number of good bytes received. This also includes local and dropped packets.
- **Total Rx** The number of bytes received, good and bad.
- **Unicast Rx/Tx** The total number of good packets that were received by and directed to a unicast address. Note that this does not include dropped unicast packets
- **Multicast Rx/Tx** The total number of good packets that were received by and directed to a multicast address. Note that this number does not include packets directed to the broadcast address
- **Broadcast Rx/Tx** The total number of good packets that were received by and directed to a broadcast address. Note that this does not include multicast packets.

Utilization

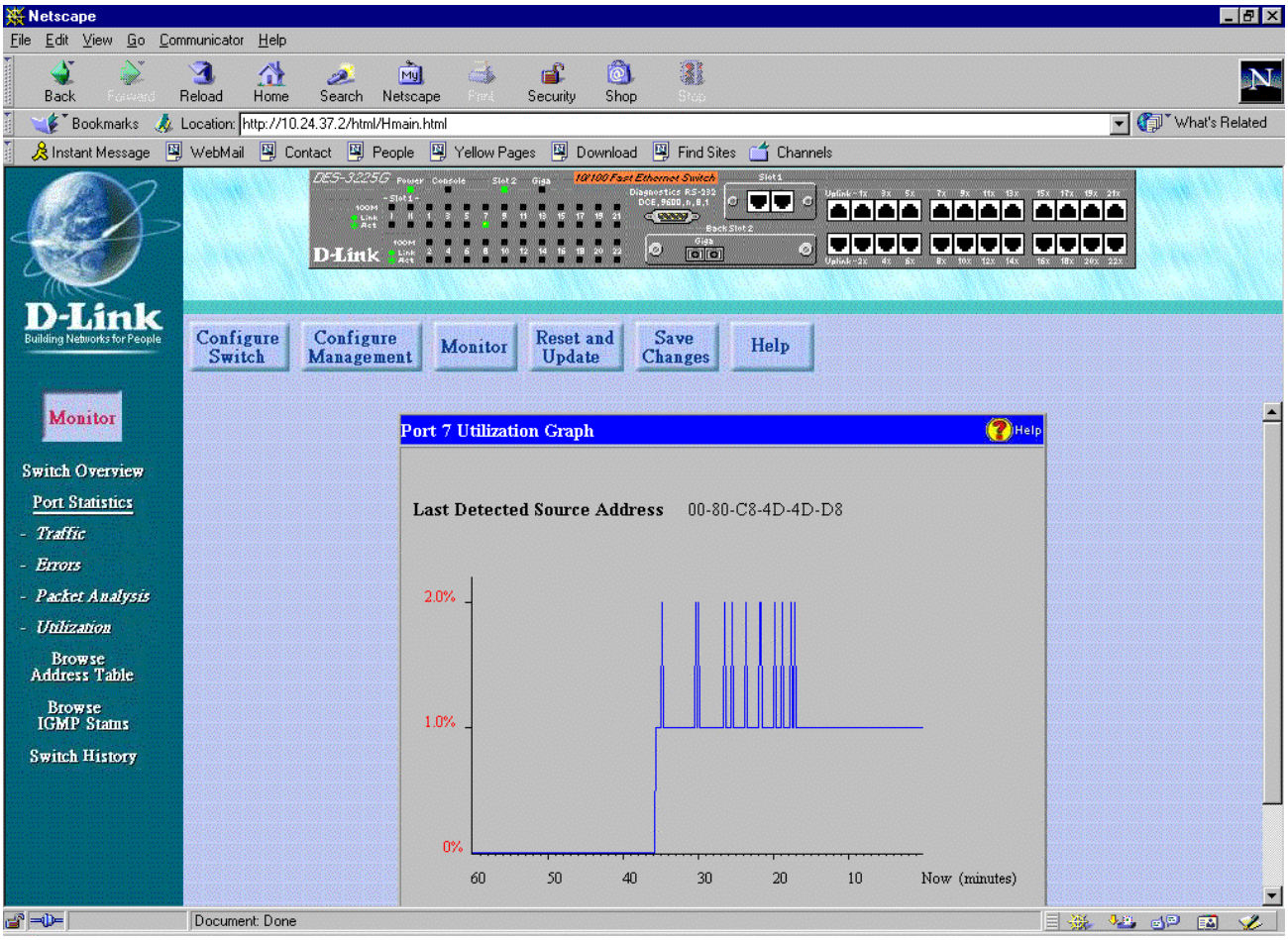


Figure 7-34. Port Utilization Graph window

The information is described as follows:

- **Last Detected Source Address** MAC address of the last device that sent packets over this port.

Browse Address Table

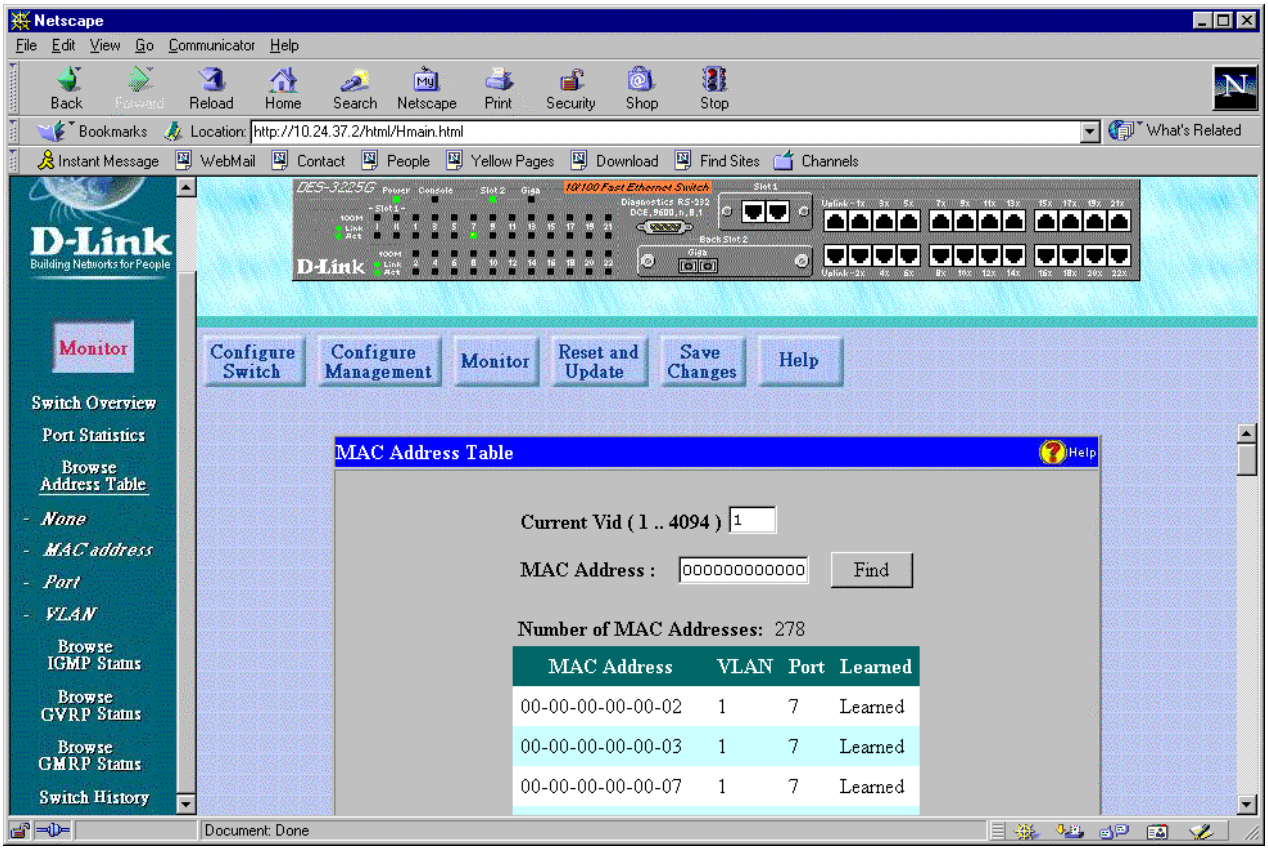


Figure 7-35. MAC Address Table window

The first selection on the Browse Address Table menu in the window on the left is None. This allows you to display a table containing MAC addresses, VLANs, ports, and respective learned statuses. Clicking the **Next Page** hyperlink at the bottom of the window will allow you to display the complete MAC Address Table. You may also enter a VLAN ID number and MAC address at the top of the table and click **Find** to locate a specific MAC Address Table entry.

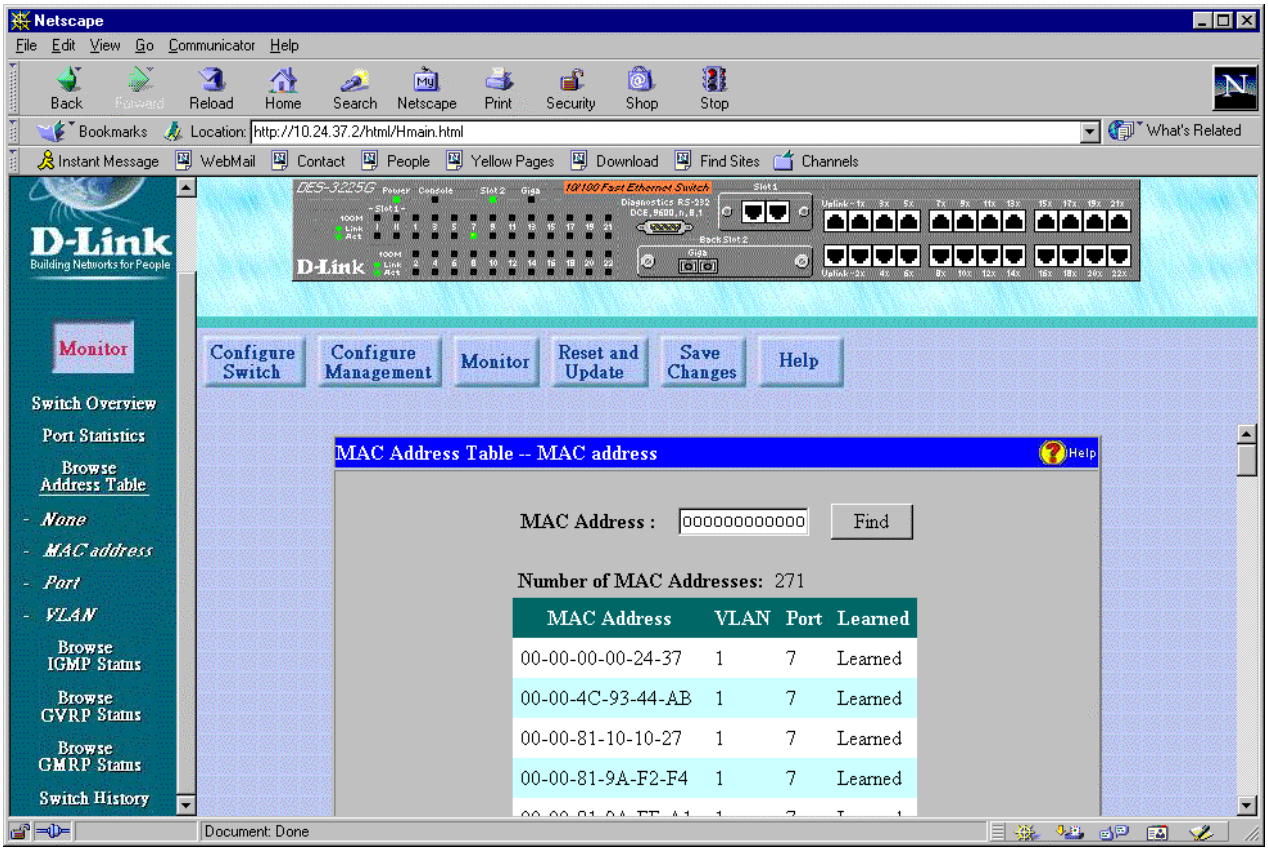


Figure 7-36. MAC Address Table – MAC address window

The second selection on the Browse Address Table menu in the window on the left is MAC Address. This allows you to display a table containing MAC addresses, VLANs, ports, and respective learned statuses. Clicking the **Next Page** hyperlink at the bottom of the window will allow you to display the complete MAC Address Table. You may also enter a MAC address at the top of the table and click **Find** to locate a specific MAC Address Table entry.

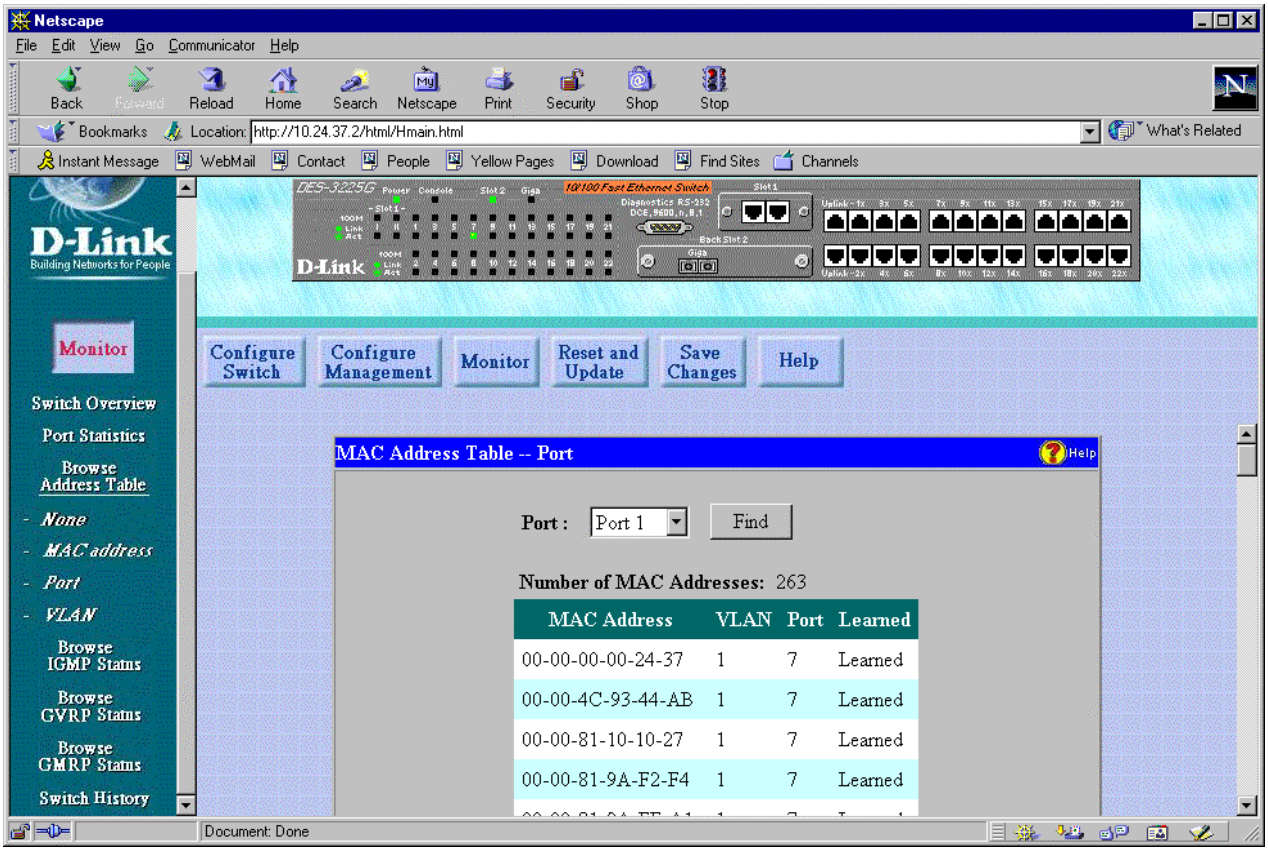


Figure 7-37. MAC Address Table – Port window

The third selection on the Browse Address Table menu in the window on the left is Port. This allows you to display a table containing MAC addresses, VLANs, ports, and respective learned statuses. Clicking the **Next Page** hyperlink at the bottom of the window will allow you to display the complete MAC Address Table. You may also enter a port number at the top of the table and click **Find** to locate a specific MAC Address Table entry.

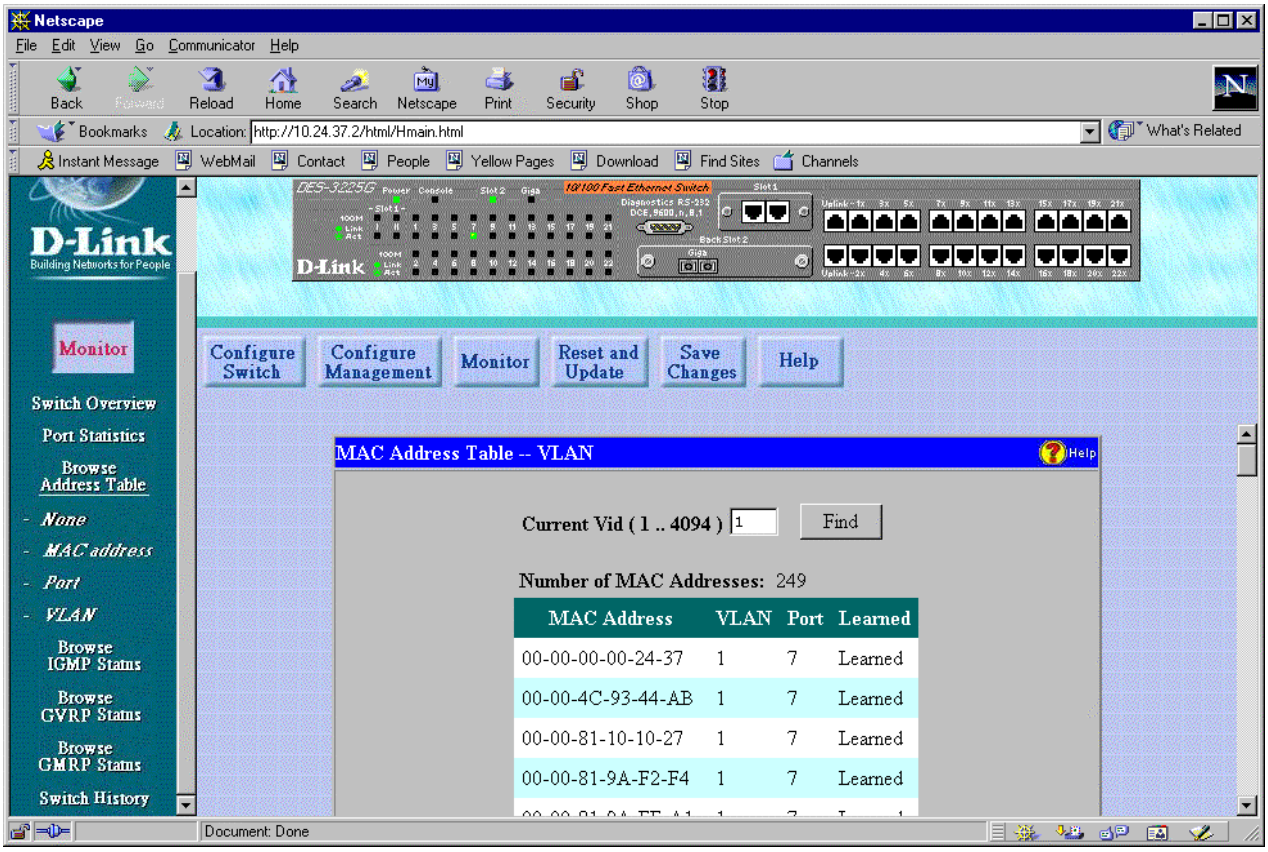


Figure 7-38. MAC Address Table – VLAN window

The fourth selection on the Browse Address Table menu in the window on the left is VLAN. This allows you to display a table containing MAC addresses, VLANs, ports, and respective learned statuses. Clicking the **Next Page** hyperlink at the bottom of the window will allow you to display the complete MAC Address Table. You may also enter a VLAN ID number at the top of the table and click **Find** to locate a specific MAC Address Table entry.

Browse IGMP Status

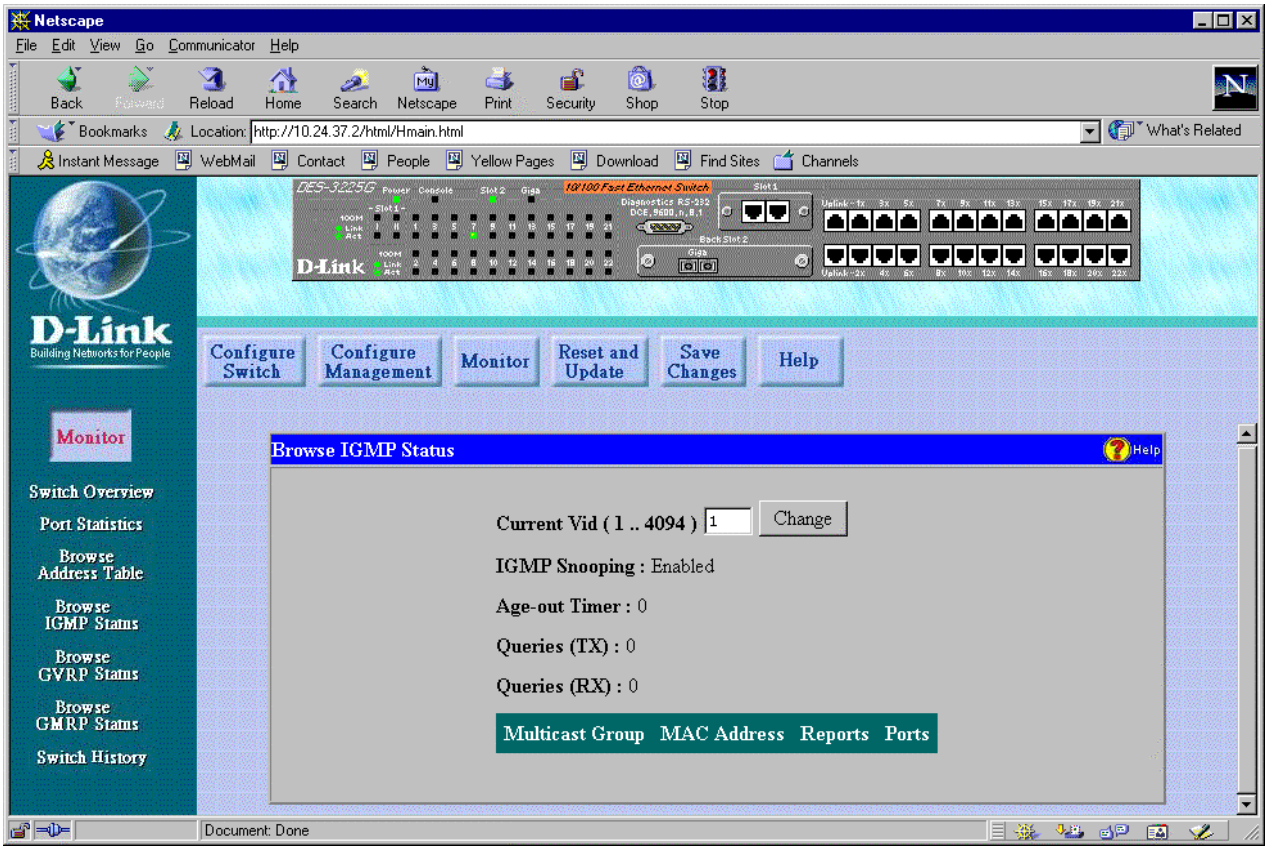


Figure 7-39. Browse IGMP Status window

This window allows you to display **Multicast Group**, **MAC Address**, **Queries (TX)**, **Queries (RX)**, **Reports**, and **Ports** for IGMP Snooping in a table format.

Browse GVRP Status

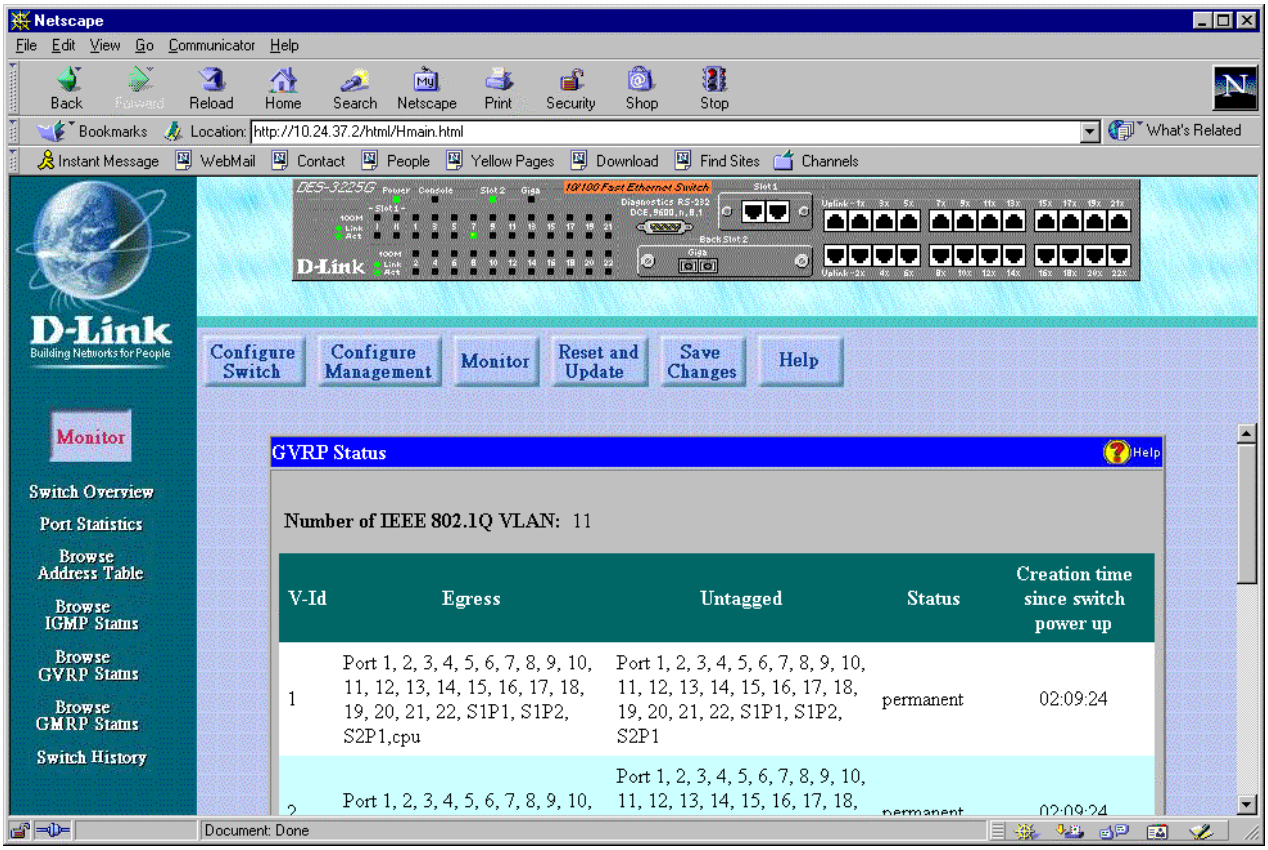

Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://10.24.37.2/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
Configure Switch
Configure Management
Monitor
Reset and Update
Save Changes
Help
Monitor
Switch Overview
Port Statistics
Browse Address Table
Browse IGMP Stats
Browse GVRP Stats
Browse GMRP Stats
Switch History
GVRP Status
Help
Number of IEEE 802.1Q VLAN: 11
V-Id
Egress
Untagged
Status
Creation time since switch power up
1
Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, S1P1, S1P2, S2P1,cpu
Port 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, S1P1, S1P2, S2P1
permanent
02:09:24
Document: Done

Figure 7-40. GVRP Status window

This window offers various pieces of information pertaining to GVRP status.

Browse GMRP Status

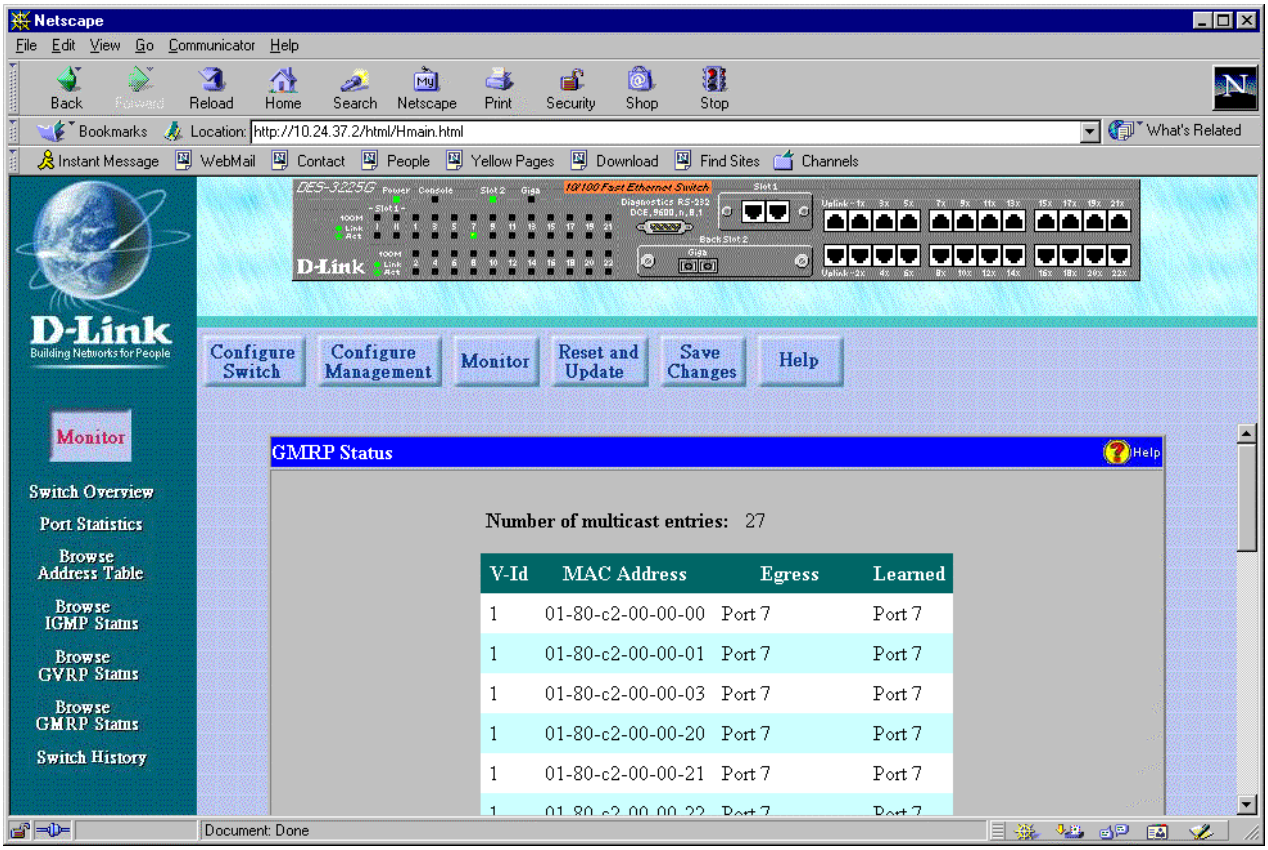


Figure 7-41. GMRP Status window

This window offers various pieces of information pertaining to GMRP status.

Switch History

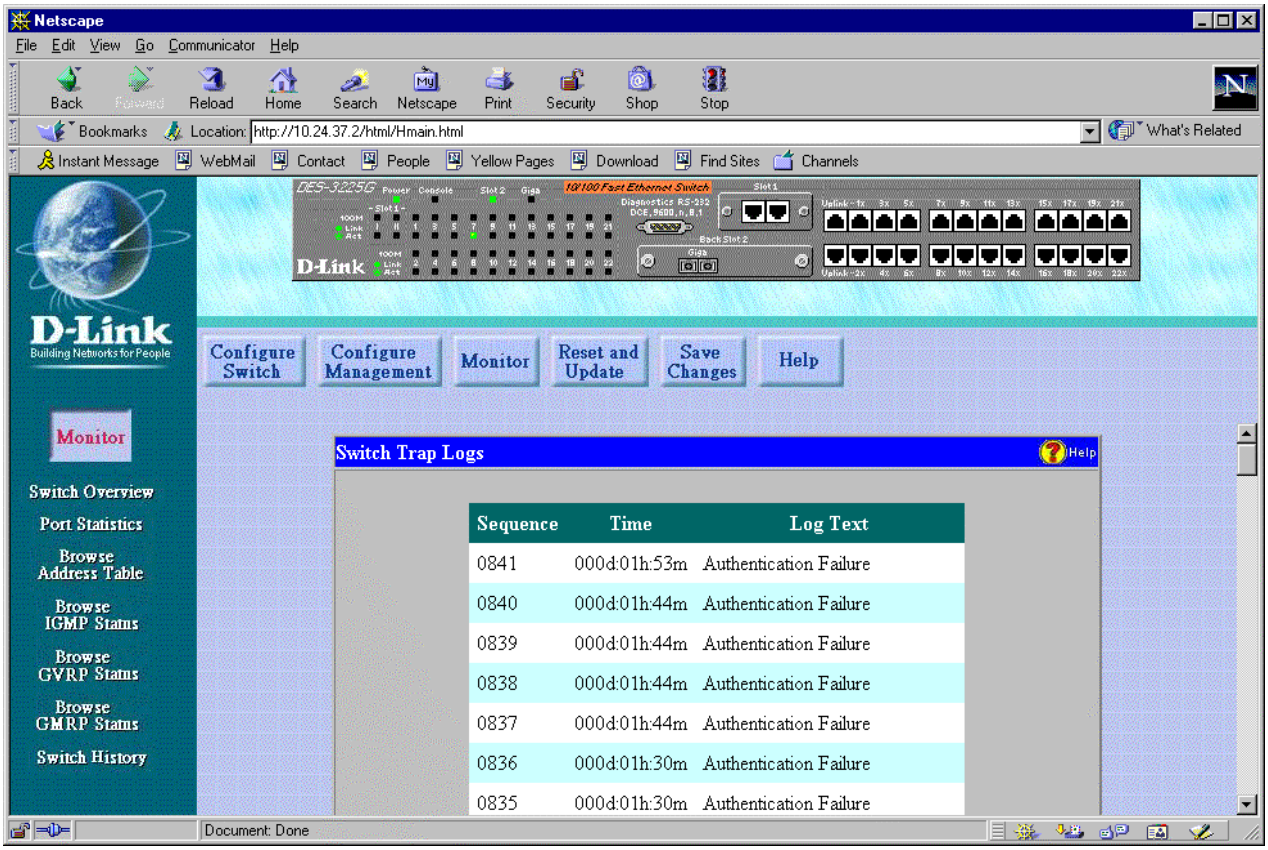


Figure 7-42. Switch Trap Logs window

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Clicking the **Next Page** hyperlink at the bottom of the window will allow you to display all the Switch Trap Logs.

The information is described as follows:

- **Sequence** Order in which each log entry was received.
- **Time** The time the log entry was received.
- **Log Text** Event information pertaining to each log entry.

Reset and Update

The fourth category includes: **Reboot Switch**, **Reset to Factory Default**, **Update Firmware**, **Change Configuration File**, **Save Settings to TFTP Server**, and **Upload Log File**.

Reboot Switch

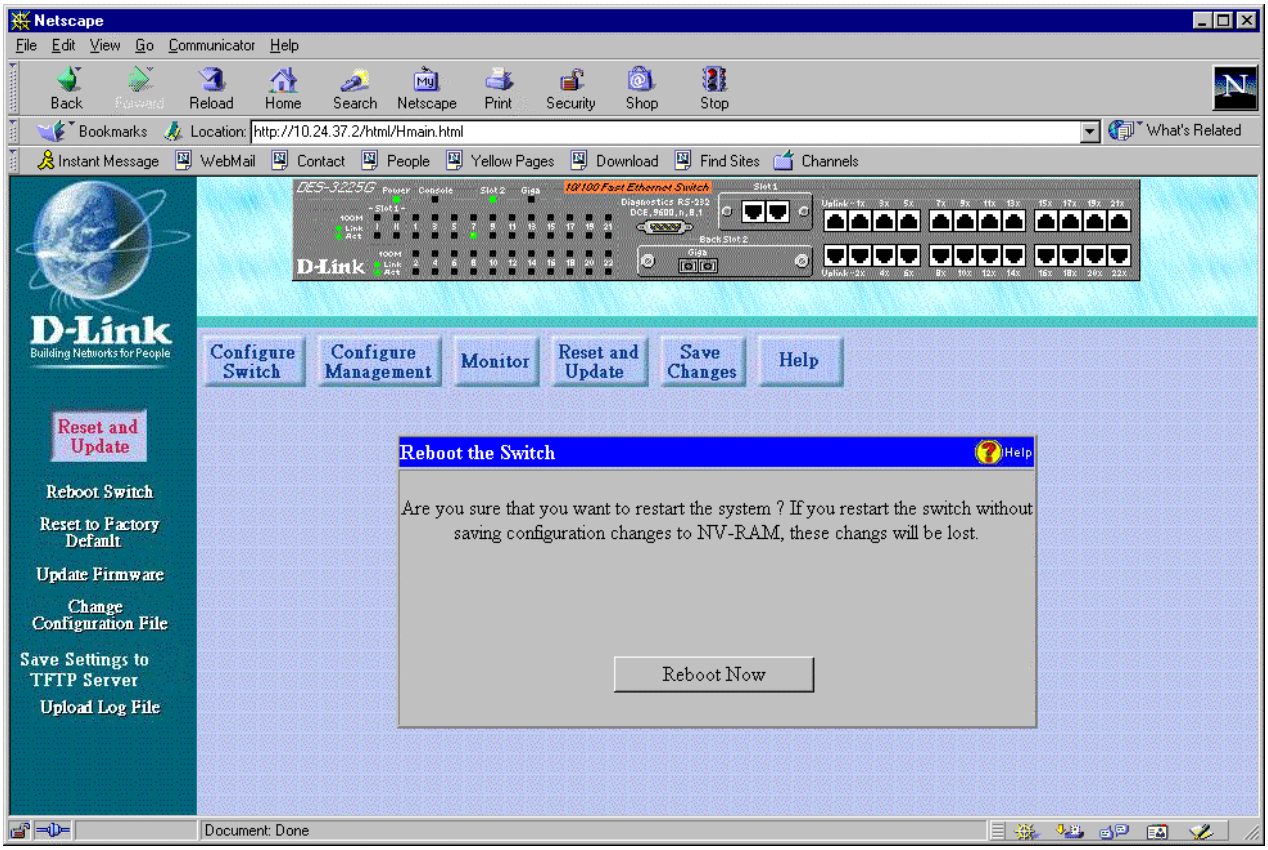

Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://10.24.37.2/html/Hmain.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
D-Link
Building Networks for People
Configure Switch
Configure Management
Monitor
Reset and Update
Save Changes
Help
Reset and Update
Reboot Switch
Reset to Factory Default
Update Firmware
Change Configuration File
Save Settings to TFTP Server
Upload Log File
Reboot the Switch
Help
Are you sure that you want to restart the system ? If you restart the switch without saving configuration changes to NV-RAM, these changs will be lost.
Reboot Now
Document: Done

Figure 7-43. Reboot the Switch window

To perform a reboot of the Switch, which resets the system, click the **Reboot Now** button.

Reset to Factory Default

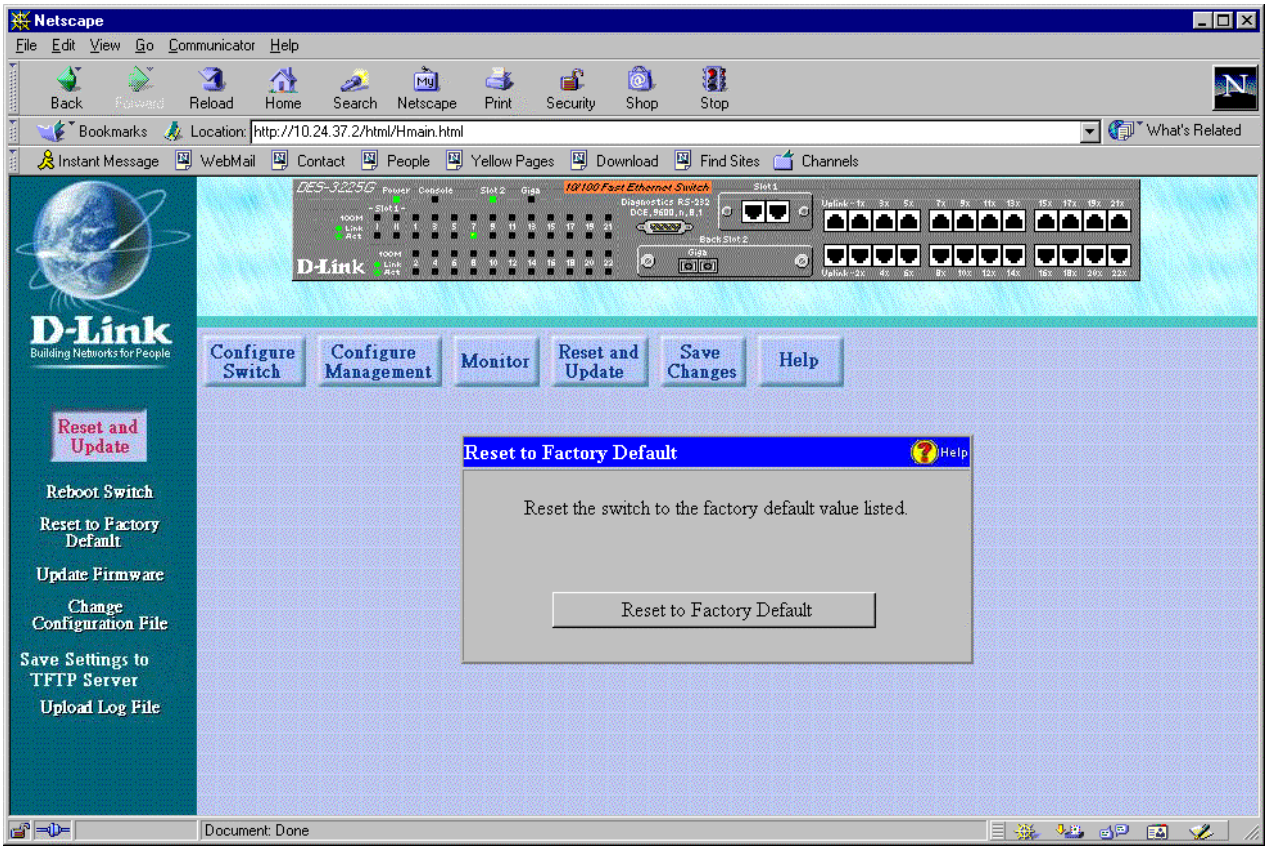


Figure 7-44. Reset to Factory Default window

A remote reset returns the Switch to the initial parameters set at the factory. Click the **Reset to Factory Default** to reset the Switch.

Update Firmware

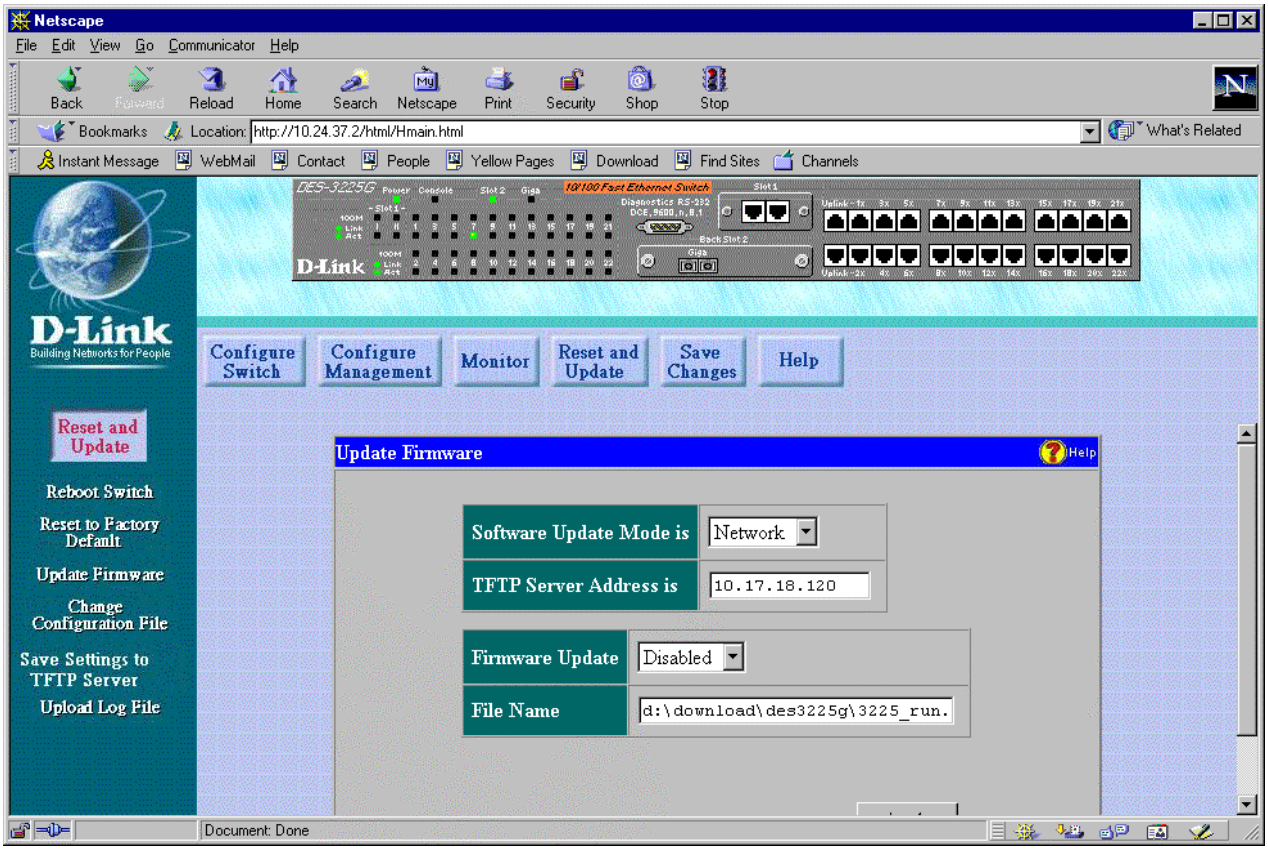


Figure 7-45. Update Firmware window

To update firmware, fill in the requested information above and then click the **Apply** button.

The information is described as follows:

- **Software Update Mode is** Set to either *Network* or *SLIP*. Determines whether the new firmware code should be obtained through the Ethernet network or through the console port.
- **TFTP Server Address** The IP address of the TFTP server where the new firmware code is.
- **Firmware Update** Determines whether or not the Switch should replace its switching software the next time it is rebooted.
- **File Name** The path and the name of the file which holds the new firmware code on the TFTP server.

Change Configuration File

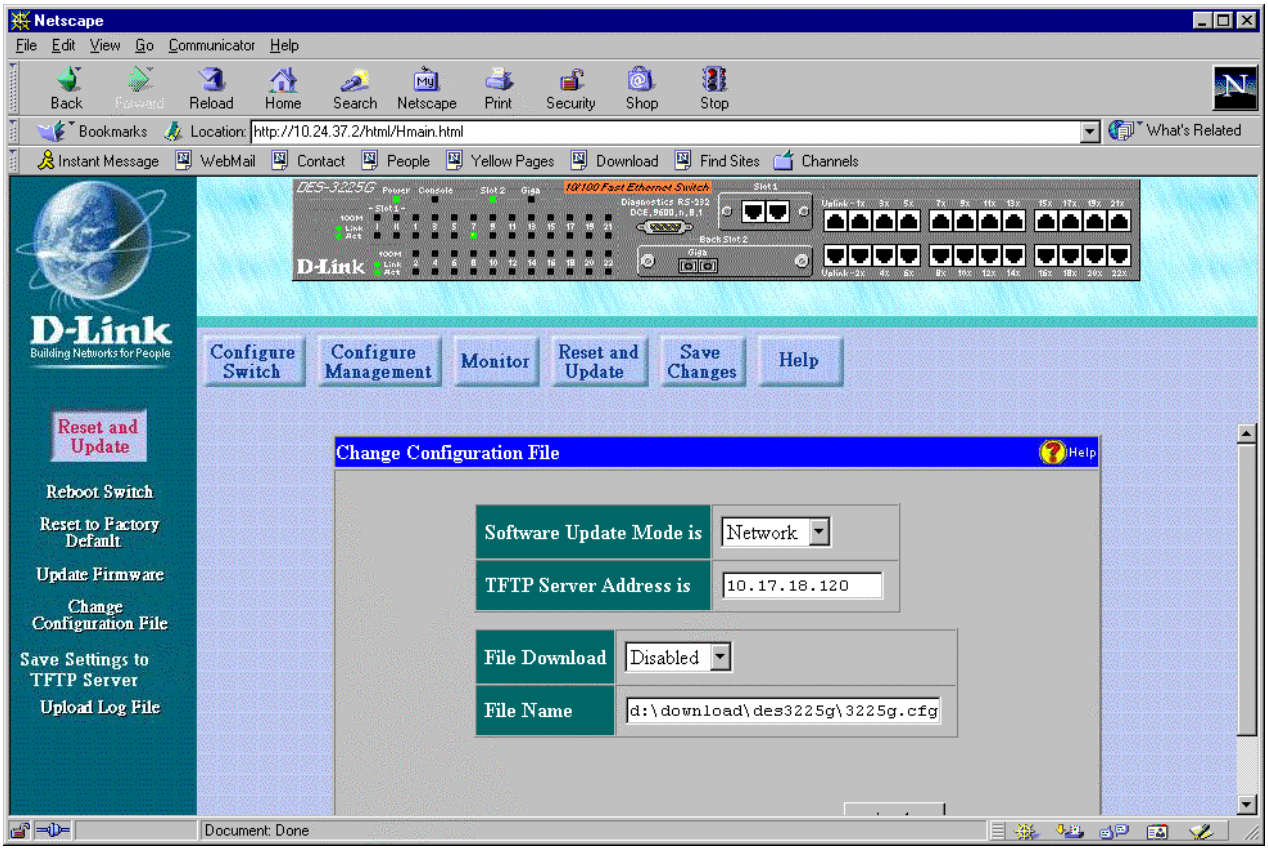


Figure 7-46. Change Configuration File window

To change a configuration file, fill the fields in above and then click **Apply**.

The information is described as follows:

- **Software Update Mode is** Set to either *Network* or *SLIP*. Determines whether the configuration file should be obtained through the Ethernet network or through the console port.
- **TFTP Server Address is** The IP address of the TFTP server where the configuration file is.
- **File Download** Determines whether or not the Switch should download its configuration file the next time it is booted.
- **File Name** The path and configuration name on the TFTP server.

Save Settings to TFTP Server

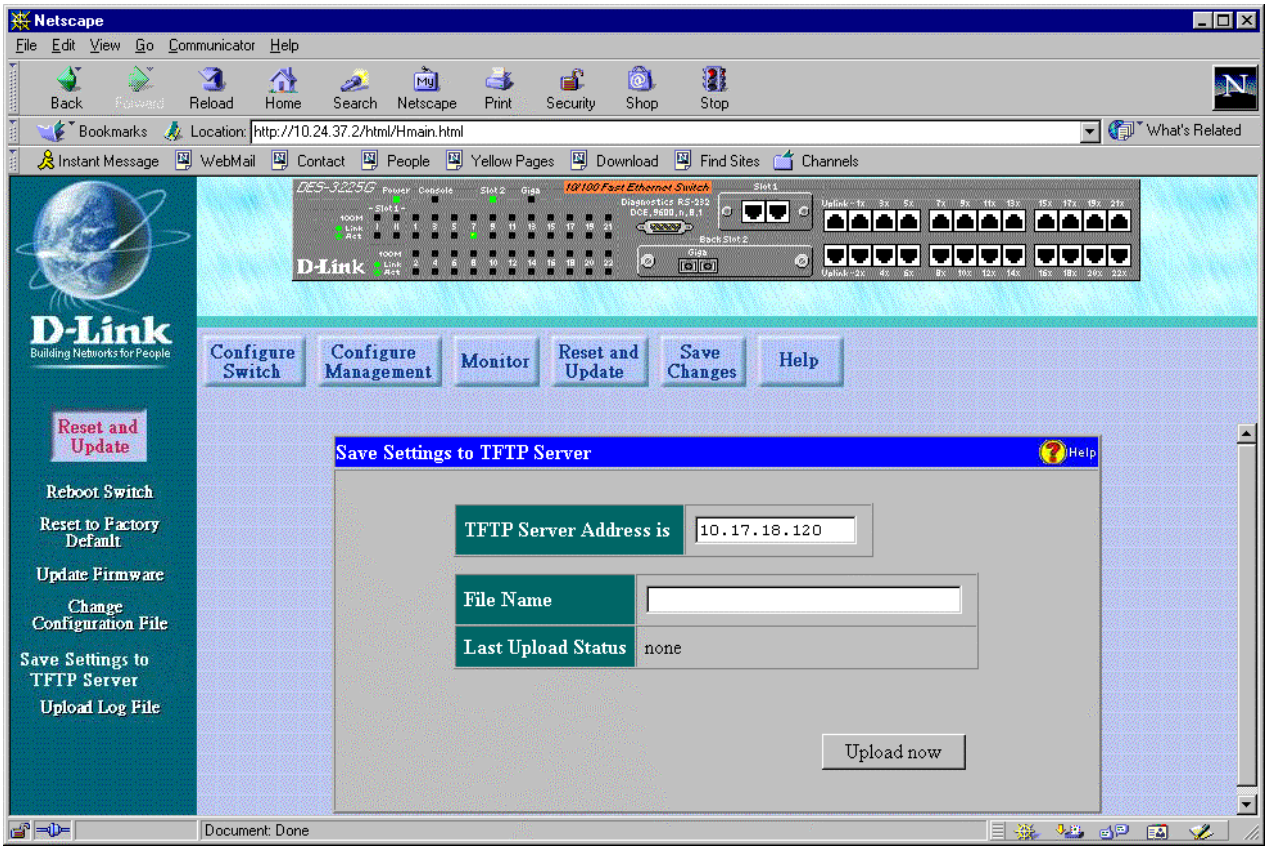


Figure 7-47. Save Settings to TFTP Server window

To save settings to a file on your TFTP server, fill the fields in above and then click **Upload now**.

The information is described as follows:

- **TFTP Server Address is** The IP address of the TFTP server where the setting file will be saved.
- **File Name** The path and file name for the settings file on the TFTP server.
- **Last Upload Status** Read-only field displays the most recent upload activity.

Upload Log File

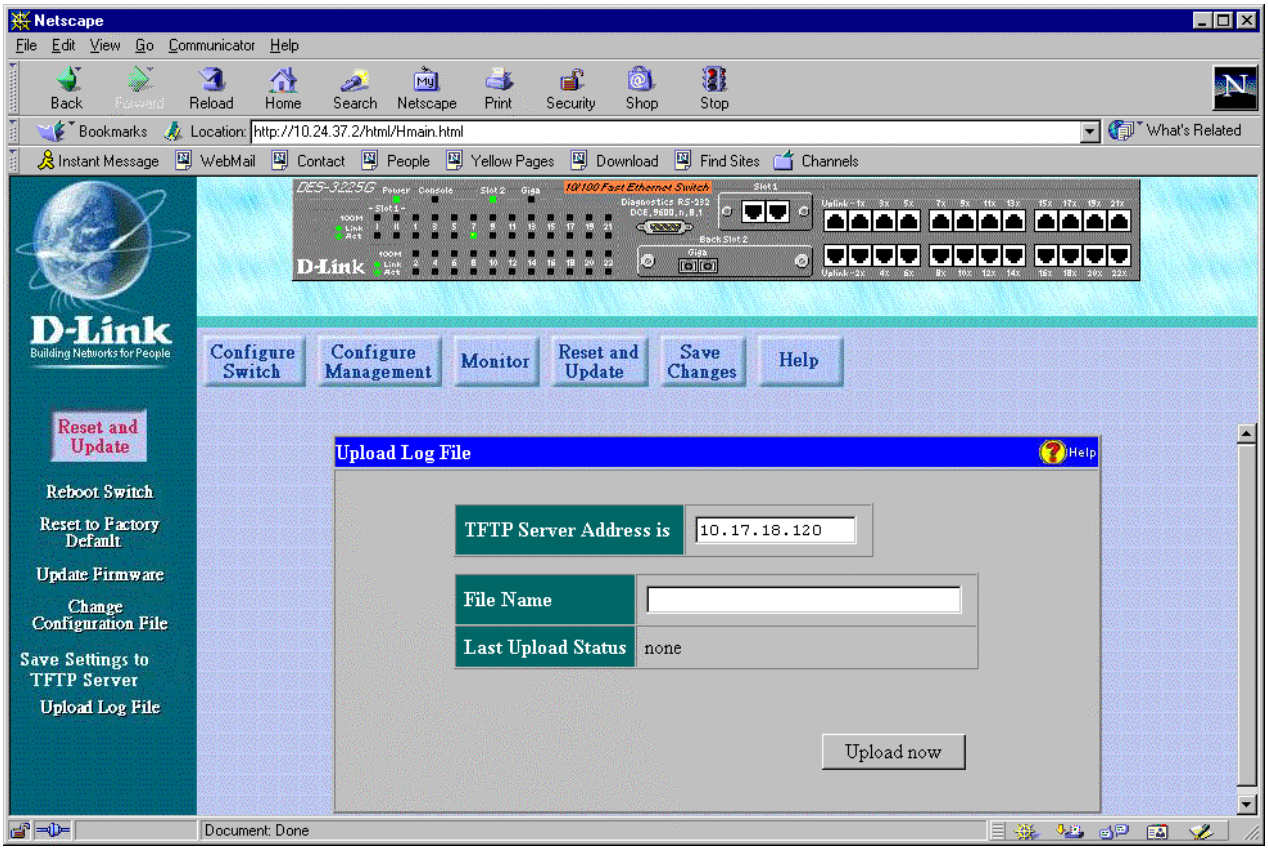


Figure 7-48. Upload Log File window

To save a log file to your TFTP server, fill the fields in above and then click **Upload now**.

The information is described as follows:

- **TFTP Server Address is** The IP address of the TFTP server where the log file will be saved.
- **File Name** The path and file name for the file to be saved on the TFTP server.
- **Last Upload Status** Read-only field displays the most recent upload activity.

Save Changes

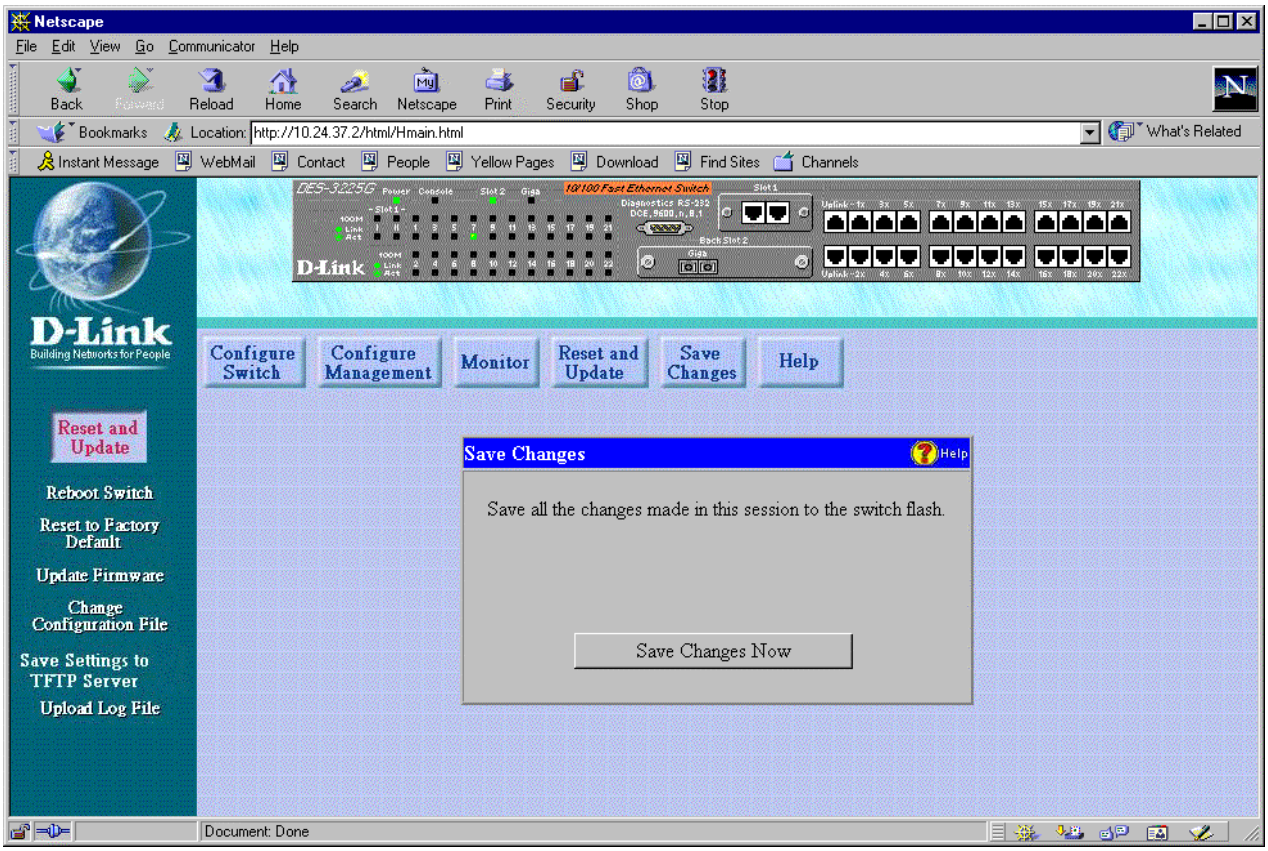


Figure 7-49. Save Changes window

To save all the changes made in the current session to the Switch's flash memory, click the **Save Changes Now** button.

Help

Click this button to access the online help files for the Switch.

A

TECHNICAL SPECIFICATIONS

General		
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX/LX Gigabit Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet ANSI/IEEE Std 802.3 NWay Auto-Negotiation IEEE 802.1Q VLAN Tagging IEEE 802.1p Priority Queue, GARP, GMRP IEEE 802.3x Full-duplex Flow Control	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half duplex	Full duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	* N/A	2000Mbps
	* 1000BASE-T can be negotiated to 1000M/Half	
Topology:	Star	

General	
Network Cables:	
10BASE-T:	2-pair UTP Cat. 3, 4, 5 (100m max.)
	EIA/TIA- 568 100-ohm STP (100 m max.)
100BASE-TX:	2-pair UTP Cat. 5 (100m max.)
	EIA/TIA-568 100-ohm STP (100m max.)
100BASE-FX:	62.5/125-micron multimode fiber (2 km max.)
1000BASE-SX:	62.5/125-micron multimode fiber (275m max.)
	50/125-micron multimode fiber (550m max.)
1000BASE-LX:	62.5/125-micron multimode fiber (550m max.)
	50/125-micron multimode fiber (550m max.)
	9-micron single-mode fiber (5 km max.)
1000BASE-T:	UTP Cat. 5 or 5e (100m max.)
	EIA/TIA-568B 100-ohm STP (100m max.)
Number of Ports:	24 x 10/100 Mbps NWay ports
	1 Gigabit Ethernet (optional)

Physical and Environmental	
AC inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption :	100 watts maximum
DC fans:	2 built-in 40 x 40 x 10 mm fans
Operating Temperature :	0 to 50 degrees Celsius
Storage Temperature :	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 367 mm x 44 mm, (17.36 x 14.45 x 1.75 inches), 19-inch standard rack-mount width (1 U)
Weight:	5 kg (11 lb.)
EMI:	FCC Class A, CE Class A, VCCI Class A, BSMI Class A, C-Tick Class A
Safety:	UL, CSA, TUV/GS

Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	12 MB per device
Filtering Address Table:	12K MAC address per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age: 10–1000000 seconds. Default = 300.

B

RJ-45 PIN SPECIFICATION

When connecting the DES-3225G Series Switch to another switch, bridge, or hub, a modified crossover cable is necessary. Please review these products for matching cable pin assignment.

The following diagram and table show the standard RJ-45 receptacle/connector and their pin assignments for the switch-to-network adapter card connection, and the straight/crossover cable for the Switch-to-switch/hub/bridge connection.

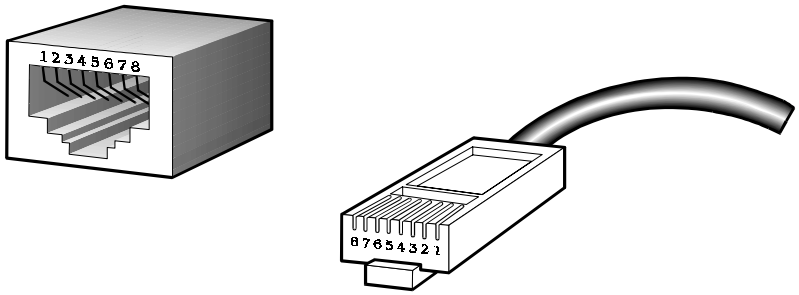


Figure B-1. The standard RJ-45 receptacle/connector

RJ-45 Connector pin assignment	
Contact	Media Direct Interface Signal
1	Tx + (transmit)
2	Tx - (transmit)
3	Rx + (receive)
4	Not used
5	Not used
6	Rx - (receive)
7	Not used
8	Not used

Table B-1. The standard Category 3 cable, RJ-45 pin assignment

The following shows straight cable and crossover cable connection:

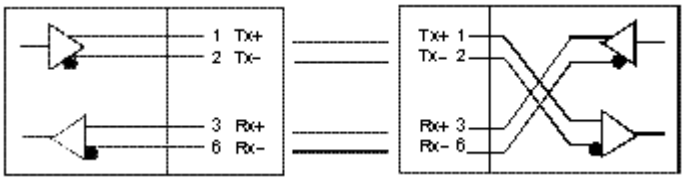


Figure B-2. Straight cable for Switch (uplink MDI-II port) to switch/Hub or other devices connection

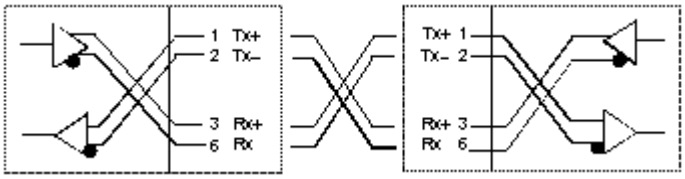


Figure B-3. Crossover cable for Switch (MDI-X port) to switch/hub or other network devices (MDI-X port) connection

C

SAMPLE CONFIGURATION FILE

This Appendix provides a sample configuration file that can be used with the **Update Firmware and Configuration Files** screen in the console program.

The configuration file is a simple text file that you create. It has two functions: to point to the location of a file on a TFTP server, and to set the IP address, subnet mask, and default gateway for the switch. The file being uploaded can be either new runtime switching software, or a switch settings file which was previously saved on the TFTP server using the **Save Settings to TFTP Server** option in the **System Utilities** menu. The IP address settings defined in the configuration file will override all other IP settings, even those defined in the settings file being uploaded. This enables the settings from one switch to be uploaded to another switch without their IP settings being the same (and thus coming into conflict).

Commands:

- `Code_type` – This command tells the Switch the type of file you wish to upload to the Switch. Possible Code_types are `PROM`, `RUNTIME`, or `CONFIG`. This should always be the first setting.
    - PROM – PROM update file.
    - RUNTIME – Switching software update file.
    - CONFIG – Image file of switch settings created by the settings backup procedure.
- `Image_file` – This command tells the Switch the complete path and filename for the file to be loaded into the Switch. For example, "`e:\3225\3225prom.tfp`". Make sure double-quotes are used as in the example file below.
- `Ip_addr` – This is the IP address that will be assigned to the switch. This command is included for downloading a configuration settings file to another switch. The IP address defined in this file will override the IP address in the configuration settings file, thus the switch you are downloading to can have a different IP address than the one that created the configuration settings file. An example IP address is `10.12.19.102`.
- `Subnet_mask` – This is the subnet mask that will be assigned to the switch. An example subnet mask is `255.128.0.0`.
- `Default_gateway` – This is the default gateway IP that will be assigned to the switch. An example default Gateway IP is `10.254.254.253`.
- # – Remark. When placed as the first character on a line, the entire line will be ignored by the switch. This allows items to be labeled, or unused commands to remain in the file so that the syntax will not be forgotten.

Notes about the Configuration File:

This configuration file can only contain 4 settings: `Code_type`, `Ip_addr`, `Subnet_mask` and `Default_gateway`.

Each command can only appear once in the configuration file.

If both the Firmware Update and Use Config File options are enabled on the **Update Firmware and Configuration Files** screen, the Firmware Update command will take precedence and only the firmware file will be uploaded to the Switch.

The Config image file, which contains all configuration settings and was created by the Switch, is prefixed with the version number of the runtime software to help with file management.

```
# Sample Config File

Code_type=PROM
Image_file="e:\3225\3225prom.tfp"

# specify IP address
Ip_addr = 10.12.19.102

# specify subnet mask
Subnet_mask = 255.128.0.0

# specify default gateway
Default_gateway = 10.254.254.253
```

D

RUNTIME SWITCH SOFTWARE DEFAULT SETTINGS

Load Mode	Ethernet
Configuration update	Disable
Firmware update	Disable
Out-of-band baud rate	9600
RS232 mode	Console
IP address	0.0.0.0
Subnet mask	0.0.0.0
Default router	0.0.0.0
BootP service	Enable
TFTP server IP address	0.0.0.0
IGMP time out	300 secs
IGMP capture state	Disable
Partition mode	Enable
Address table lock	Disable
Device HOL	Enable
Port HOL	Enable
Console time out	15 min
User name	Blank
Password	Blank
Device STP	Disable
Port STP	Enable
Port enable	Enable
Bridge max age	20 secs
Bridge hello time	2 sec
Bridge forward delay	15 sec
Bridge priority	32768
Port STP cost	19 (Gigabit=4)
Port STP priority	128
Forwarding table aging time	300 secs
Address lookup mode	Level 1
NWay	Enable`
Flow control	Enable
Backpressure	Disable
Port lock	Disable
Port priority	Default
Broadcast storm rising action	Do nothing
Broadcast storm falling action	Do nothing
Broadcast storm rising threshold	500pkts/sec
Broadcast storm falling threshold	250pkts/sec
Community string	"public", "private"
VLAN mode	Basic
SNMP VLAN(802.1Q)	1
Default port VID	1
Ingress rule checking	Disable
Mirror src port <->target port	1←2
Mirror	Disable

INDEX

10BASE-T Device 13
64 89
65-127 89
100BASE-FX (MT-RJ Type) Fiber Module 9
100BASE-FX (SC) Fiber Module 9
100BASE-TX Device 13
100BASE-TX Module 9
100M 11
100Mbps Fast Ethernet 1
128-255 89
256-511 89
512-1023 89
802.1Q VLAN Segmentation 23
802.1Q VLANs 22
802.1Q VLANs Spanning Multiple Switches 24
1000BASE-LX Gigabit Module 10
1000BASE-SX Gigabit Module 10
1000BASE-T Copper Gigabit Module 11
1024-1518 89

A

AC inputs 152
AC power cord 4
Access Rights
  read only 83
  read/write 83
Accessory pack 4
Add/Modify User Accounts 33
Address Table Lookup Mode 49
Administrator 30
Advanced Settings 39
Age-out Timer 55, 91
Aging Time, definition of 17
Aging Time, range of 17
Alleviating network loop problems 19
APPLY 28
Apply button 30
Auto polarity detection 3
Automatic learning 17
auto-negotiate 2

B

Baud Rate 37
Block 41
BOOTP (BOOTstrap Protocol) 77
BOOTP protocol 36
BOOTP server 36
BPDU 47
Bridge Forward Delay 19
Bridge Hello Time 19
Bridge Identifier 18
Bridge Max. Age 19
Bridge MIB (RFC 1493) 3
Bridge Priority 18, 19, 20
Broadcast Rx (Broadcast Frames Received) 90
Broadcast Storm Falling Action 41
Broadcast Storm Falling Threshold 41
Broadcast Storm Rising Action 41
Broadcast Storm Rising Threshold 41
Browse Address Table 90
Browse GMRP Status 93
Browse GVRP Status 92
Browse IGMP Status 91
Bytes Recv 87
Bytes Sent 87

C

Changing the Protocol Parameters 45, 48
Changing the SNMP Manager Configuration parameters settings 83
Changing your Password 31
Collisions 89
Community Name 15
Community name, definition of 82
Community names
  Private 82
  Public 82
Config File Name 78
Configuration 34
Configure 802.1Q IGMP 52
Configure Filtering and Forwarding Table 48
Configure IGMP Filtering 51
Configure IP Address 35
Configure MAC Address Filtering 51
Configure Port Mirroring 44
Configure Port VLAN ID 66
Configure Ports 39
Configure Slot1 Module 41
Configure Slot2 Module 43
Configure Static Forwarding Table 49
Configure Static VLAN Entry 66
Configure Switch 38
Configure Trunk 76
Configure VLANs & MAC-based Broadcast Domains 55
Connections
  Switch to End Node 12
  Switch to Hub or Switch 12
console 27, 28
Console 11
console port 3, 7
Console port (RS-232 DCE) 14
Console port settings 14
Console Timeout 37
CRC Error 88

CRC Errors 86, 87
Create/Modify User Accounts 31
Create/Remove a MAC-based VLAN 58
crossover cable 13
Crossover cable 155
Current VLAN Mode 57

D

Data filtering 3
Data filtering rate 3
Data forwarding 3
Data forwarding rate 3
data packet 47
Default Gateway 36
Designated Bridge 18
Designated Port 18
Destination IP Address 80
Diagnostic port 3
Dimensions 152
disabling a port 43
Displaying Forwarding Table entries 49
Displaying Port Statistics 91, 92
Dropped Frames 89
Dynamic filtering 17
Dynamic Filtering, definition of 48

E

Egress 71
Egress port 24
End Node 12
Entity MIB, version (RFC 1757) 3
Ethernet protocol 1
events 15

F

factory reset 31
Factory Reset 94, 95
Factory Reset NV-RAM to Default Value 95
Fast Ethernet Technology 1
File Name 78
Filtering 17
Firmware Update 78
Flash memory 3
Flow Control 40
Forward 41, 43, 44
Forward Delay 20
Fragments 88
Frames Recv. 87
Frames Sent 87
Front Panel 7
Full-duplex 3

G

gateway router 15
General User 30
Giga 11
Gigabit Ethernet 1, 7
Group name 77

H

half-duplex 3
Head Of Line (HOL) Blocking Prevention 39
Head-of Line blocking 39
Hello Time 20
Humidity 152

I

IEEE 802.1p/Q priority tag 41
IEEE 802.1Q port-based VLAN 66
IEEE 802.1Q VLANs 52
IGMP packets 51
IGMP query and report packets 54
IGMP snooping 51
IGMP Snooping 91
Illustration of STA 19
Ingress Filtering 66
Ingress port 24
Internet Group Management Protocol (IGMP) 51
IP address 36, 83
IP Address 15
IP Addresses and SNMP Community Names 15
IP Configuration 35
IP Multicast Filtering (IGMP Snooping) 52
IP Multicast Filtering Age-out Timer 52, 75

J

Jabber 88

L

Last Seen MAC 87
Late Collisions 88
LED Indicators 11
Link/Act 11
load-balancing 21
Local console management 14
Lock Address Table 49
log in 31
Logging on 28
Logout 96

M

MAC Address 50, 61, 92
MAC Address Aging 49
MAC address filtering 17
MAC Address Learning 153
MAC Rx Errors (MAC Received Errors) 88
MAC-based Broadcast Domains 22
MAC-Based VLAN-MAC Assignment 60
MAC-based VLANs 57
Main Menu 29
Management 3
Management Information Base (MIB) 16
Management VID 68, 118
Master 77
master port 20
Max. Age 19, 47

Max. Age Time 20
MIB 16
MIB objects 16
MIB-II 16
MIB-II (RFC 1213) 3
MIBs 16
mirror port 45
module 2, 7
Modules 8
Multicast Group 92
Multicast Rx (Multicast Frames Received) 90
Multicasting 51

N

Network Classes
  Class A, B, C for Subnet Mask 36
Network Monitoring 84
network performance 39
not apply 50
Not-Apply 61
NV-RAM 31, 95
NWay 2

O

Operating Temperature 152
Out-of-band management and console settings 37
Out-of-Band/Console Setting menu 37
Oversize Frames 88

P

Packet Forwarding 16
packet queues 40
partition 39
Path Cost 18
Performing a System Reset 94
Ping Test 79
Port 40, 50
  partition 39
Port Auto-Partition Capability on All Ports 39
Port Level, STA Operation Level
  Path Cost 18, 48
Port Lock 41
Port Mirroring 44
Port Packet Analysis Statistics 89
Port Packet Error Statistics 88
Port Priority 18, 19, 20
Port Traffic Statistics 86
Port Trunking 20
Port type settings
  Console 37
  Out-of-Band 37
Port VLAN ID numbers (PVIDs) 66
Port-based VLANs 25
ports 2
Ports 92
Power 11
Power Consumption 152
Priority 40
priority queue 40
priority tag 41
Proprietary MIBs 3

Q

Queries(RX) 92
Queries(TX) 92

R

RAM 31
RAM Buffer 153
Rear Panel 7, 8
refresh 28
Repetitions 80
Reports 92
Resetting the Switch 94
Restart System 94
Restart VLAN Mode 57
RJ-45 Pin Specification 154
RMON MIB (RFC 1757) 3
RMON probe 44
Root Bridge 18
Root Path Cost 18
root port 47
Root Port 18
Routers 2
RS-232 3
RS-232 DCE console port 14
Rx (Good) (Frames Received) 89
RX Octets 90
RX/sec 86

S

Save Changes 28
Save Settings to TFTP Server 80
Save Switch History to TFTP Server 81
Saving Changes 30
security 15
Segments, Network 2
Serial Port 37
Server IP Address 81
Setting Up The Switch 34
Setup 4
Sharing Resources Across 802.1Q VLANs 23
SLIP management 37, 130
Slot 2 11
sniffer 44
SNMP Community String 83
SNMP Manager Configuration 82
SNMP Manager Configuration parameter
  Status 83
SNMP Security (Community Names) 82
SNMP Trap Manager Configuration 82
Software Update menu 77
Software Updates 77
Spanning Tree Algorithm 3
Spanning Tree Algorithm (STA) 17
Spanning Tree Algorithm Parameters 45

Custom Filtering Table 51, 74
Forwarding Table 49
Protocol Parameters 45
Spanning Tree Protocol 17
Speed 87, 88
Speed/Duplex 40
STA Operation Levels 18
Static Filtering, definition of 48
Static filters 50
static forwarding entries 51
Static Multicast Filtering Table 75, 76
Storage Temperature 152
Store and forward switching 3
STP Port State 41
straight cable 155
subnet mask 99
Subnet Mask 36
Super User 30
switch 2
Switch History 93
Switch Management 14–26
Switch Monitoring 83
Switching Technology 2
System Contact 38
System Location 38
System Name 38
System Restart Setting
Out-of-Band Baud Rate 130
System Utilities 78

T

Tag/Untag 71
Tagging 66
Tagging 24
TCP/IP Settings 35
Telnet 27
TELNET program 28
TFTP (Trivial File Transfer Protocol) 77
TFTP Server Address 78
Third-party vendors' SNMP software 16
Total Bytes Recv 87
Total Bytes Rx (Total Bytes Received) 89
Total errors 89
Total Frames Recv. 87
Total RX 90
Traffic Statistics 84
Transmission Methods 153
Trap managers 15
Trap Recipient 41
Trap Type
Authentication Failure 15
Broadcast Storm 16
Cold Start 15
Link Change Event 16
New Root 15
Port Partition 16
Topology Change 16
Warm Start 15
Traps 15
trunk group 20
trunk ports 21
Tx (Good) (Frames Sent) 89
TX Octets 89
TX/sec 86

U

unauthorized users 28
Undersize Frames 89
Unicast RX/Unicast TX 90
Unpacking 4
Untagging 66
Untagging 24
Update Firmware and Configuration Files 77
Uplink 7, 13
Use Configuration File 78
User Accounts Management 32
utilization 41, 43, 44

V

VID 54, 71
View/Delete User Accounts 33
VLAN 17, 66
VLAN Description 59
VLAN ID 55
VLAN ID number 69
VLAN Name 71
VLANs and Broadcast Domains 21

W

Web-based management 97
Web-based management module 97
Weight 152
Width 77

D-Link® Offices

AUSTRALIA — **D-LINK AUSTRALASIA**
Unit 16, 390 Eastern Valley Way Roseville, NSW 2069 Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE (Australia): 1800 177 100 TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au

CANADA — **D-LINK CANADA**
2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223 BBS: 1-965-279-8732 TOLL FREE: 1-800-354-6522
URL: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca

DENMARK — **D-LINK DENMARK**
Naverland 2 DK-2600 Glostrup Copenhagen, Denmark
TEL:45-43-969040 FAX:45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk

EGYPT — **D-LINK MIDDLE EAST**
7 Assem Ben Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-245-6176 FAX: 202-245-6192 URL: www.dlink-me.com E-MAIL: support@dlink-me.com & fateen@dlink-me.com

FRANCE — **D-LINK FRANCE**
Le Florilege #2, Allee de la Fresnerie, 78330 Fontenay le Fleury, France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.com E-MAIL: info@dlink-france.fr

GERMANY — **D-LINK GERMANY**
Bachstrae 22, D-65830 Kriftel, Germany
TEL: 49-(0)6192-97110 FAX: 49-(0)6192-9711-11 URL: www.dlink.de BBS: 49-(0)6192-971199 (analog)
BBS: 49-(0)6192-971198 (ISDN) INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free)
REPAIR: 00800-7250-8000 E-MAIL: mbischoff@dlink.de & mboerner@dlink.de

INDIA — **D-LINK INDIA**
Plot No.5, Kurla-Bandra Complex Rd., Off Cst Rd., Santacruz (E) Bombay - 400 098 India
TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: www.dlink-india.com E-MAIL: service@dlink.india.com

ITALY — **D-LINK ITALY**
Via Nino Bonnet n.6/b, 20154 Milano, Italy
TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it

JAPAN — **D-LINK TOKYO**
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141 Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp

SINGAPORE — **D-LINK INTERNATIONAL/D-LINK SINGAPORE**
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL : 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

SWEDEN — **D-LINK SWEDEN**
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-(0)8564-61900 FAX: 46-(0)8564-61901 E-MAIL: info@dlink.se URL: www.dlink.dk

TAIWAN — **D-LINK TAIWAN**
2F, No. 119 Pao-Chung Rd, Hsin-Tien, Taipei, Taiwan, R.O.C.
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 URL: www.dlinktw.com.tw E-MAIL: dssqa@tsc.dlinktw.com.tw

U.K. — **D-LINK EUROPE/D-LINK U.K.**
4th Floor, Merit House, Edgeware Road, Colindale, London NW9 5AB U.K.
TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. — **D-LINK U.S.A.**
53 Discovery Drive, Irvine, CA 92618, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033 BBS: 1-949-455-1779 & 1-949-455-9616 INFO: 1-800-326-1688
URL: www.dlink.com E-MAIL: tech@dlink.com & support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____
Organization: _____Dept. _____
Your title at organization: _____
Telephone: _____ Fax:_____
Organization's full address: _____
_____
Country: _____
Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____
Telephone: _____ Fax:_____
Reseller's full address: _____
_____
_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?
☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?
☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?
☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others_____

5. What network management program does your organization use ?
☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others_____

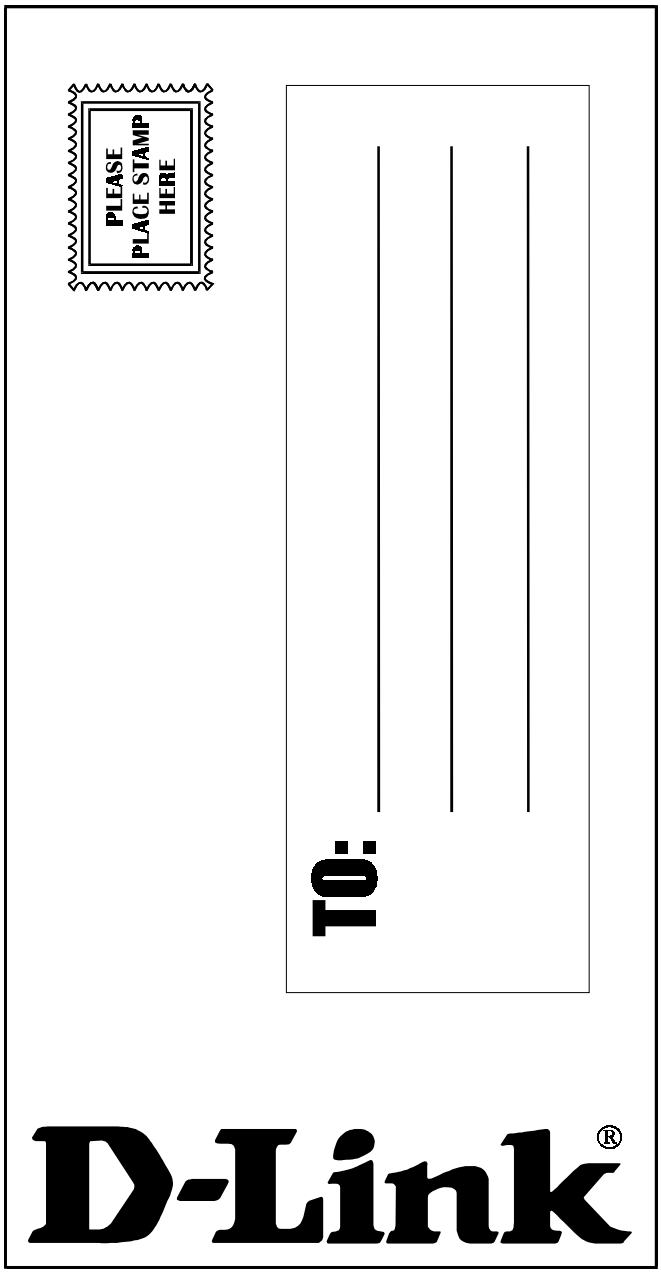
6. What network medium/media does your organization use ?
☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?
☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?
☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?
☐Yes ☐No ☐Don't know yet

10.Your comments on this product?
_____
_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®